AGENCE DES SYSTÈMES D'INFORMATION PARTAGÉS DE SANTÉ

CRYPTOLIB-CPS

Manuel utilisateur

9 Février 2012

Version 2.13

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

SOMMAIRE

1. INTRODUCTION 5

2. PRESENTATION TECHNIQUE 6

2.1. CRYPTOLIB-CPS : BIBLIOTHEQUES CRYPTOGRAPHIQUES DE LA CARTE CPS 6

2.2. ARCHITECTURE DES COMPOSANTS CRYPTOLIB-CPS, API-CPS ET GALSS 8

2.3. WINDOWS : LE PROGRAMME CCM ASSOCIE A LA BIBLIOTHEQUE CSP-CPS 9

2.4. MACINTOSH : SPECIFICITES DE L'ARCHITECTURE CDSA / TOKEND 10

2.5. LES CERTIFICATS X.509 DE LA CARTE CPS 12

2.6. CHAINES DE CONFIANCE DES CERTIFICATS X.509 DE LA CARTE CPS 13

2.7. LA LOGIQUE DU PROGRAMME D'INSTALLATION (CAHIER DES CHARGES) 14

3. GUIDE D'INSTALLATION DE CRYPTOLIB 15

3.1. LES PRE REQUIS AVANT TOUTE INSTALLATION 15

3.2. INSTALLATION 16

3.3. DESINSTALLATION 17

4. GUIDE D'UTILISATION DE CRYPTOLIB 18

4.1. CONNEXION HTTPS PAR INTERNET EXPLORER (WINDOWS) 19

4.1.1. Contrôles sur l'utilitaire CCM 19

4.1.2. Connexion HTTPS 21

4.2. CONNEXION HTTPS PAR SAFARI (MACINTOSH) 23

4.2.1. Contrôles visuels de l'installation 23

4.2.2. Connexion HTTPS 25

4.3. CONNEXION HTTPS PAR MOZILLA FIREFOX (WINDOWS, LINUX, MAC-OSX) 27

4.3.1. Ajout du périphérique PKCS#11-CPS dans Firefox 27

4.3.2. Connexion HTTPS 29

5. AIDES AUX DIAGNOSTICS 31

5.1. COMPTE RENDU DE FIN D'INSTALLATION 31

5.2. AIDES AUX DIAGNOSTICS 32

5.3. LISTE DES COMPOSANTS INSTALLES 39

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5.3.1. Environnement Windows 39
5.3.2. Environnement Macintosh 42
5.3.3. Environnement Linux 46

6. TERMINOLOGIE 48

7. SUIVI DES MODIFICATIONS DU MANUEL 49

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

ILLUSTRATIONS

Figure 1 Architecture des composants CRYPTOLIB-CPS, API-CPS et GALSS 8
Figure 2 Exemple d'un certificat X.509 d'authentification d'une CPS2bis (CPA)..... 12
Figure 3 Exemples de chaînes de confiance de CPS 13
Figure 4 Organigramme de principe de l'installation 14
Figure 5 Exemple de barre des tâches sous Windows avec CCM..... 17
Figure 6 CCM : exemple d'état de deux lecteurs dont un avec une CPS 20

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

1. INTRODUCTION

Ce document constitue le manuel utilisateur des bibliothèques cryptographiques de la carte CPS.
Il est destiné aux usagers de machines Windows, Macintosh, ou Linux, équipées d'un lecteur de cartes CPS.

Le lecteur de ce document est supposé avoir reçu le programme d'installation de ces bibliothèques sur un support de type CD, ou sous la forme d'un package logiciel compressé (type ZIP sous Windows, DMG sous Mac, etc…).

Il trouvera dans ce document quatre parties principales :

- Une présentation technique de ces bibliothèques cryptographiques pour comprendre ce que va réaliser le programme d'installation.
- Un guide d'installation pour aider l'opérateur sur ses manipulations et ses choix de réponses et s'assurer du bon fonctionnement ultérieur.
- Un guide de première utilisation simple par connexion sécurisée par CPS sur un serveur de test de l'ASIP Santé.
- Une aide aux diagnostics sous forme de liste de contrôles de cette installation si des problèmes sont rencontrés.

Pour un lecteur « pressé », l'installation se résume en quatre points :

1. Disposer d'une machine Windows, Mac OS X ou Linux déjà équipée physiquement d'un lecteur soit bi-fente de type FSE, soit mono-fente NF-CPS, soit mono-fente PC/SC.
2. Terminer et arrêter toutes ses applications, dont celles qui accèdent à la carte CPS, car il faudra relancer la machine.
   En particulier, arrêter les messageries OSM, l'agent RSS…
3. Exécuter l'installation à partir du CD ou du package logiciel…
   Laisser le CD en place s'il est présent, et relancer sa machine…
4. Valider la fin de l'installation et la tester sur un navigateur.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2. PRESENTATION TECHNIQUE

2.1. CRYPTOLIB-CPS : BIBLIOTHEQUES CRYPTOGRAPHIQUES DE LA CARTE CPS

La carte CPS contient dans sa puce électronique les moyens d'effectuer des calculs cryptographiques de signature[1] ou d'authentification[2].
En première approximation, appelons ces moyens les « certificats X.509[3] ».

De plus en plus de logiciels comme les navigateurs (Internet Explorer sur Windows, Safari sur Mac OS-X ou Mozilla FireFox, etc…) ou les messageries savent manipuler et exploiter des certificats X.509. Ils le font en respectant un langage parmi les trois standards reconnus : Microsoft CryptoAPI (dans le monde Windows), Common Data Security Architecture (CDSA) d'Apple (dans le monde Macintosh), ou RSA PKCS#11 (universel).

CryptoAPI (ou CAPI) / CSP
Cryptographic Application Program Interface. CAPI est une API développée par Microsoft qui définit un jeu de fonctions cryptographiques utilisables par les applications Windows. Un module logiciel qui implémente ces fonctions se nomme un CSP pour " Cryptographic Service Provider". Un CSP doit être signé par Microsoft avant d'être utilisable.

Common Data Security Architecture (ou CDSA) / Tokend
CDSA est une architecture développée par Apple qui définit un jeu de fonctions cryptographiques utilisables par les applications Macintosh. Un module logiciel qui implémente ces fonctions se nomme un Tokend.

PKCS (Public Key Cryptography Standards) #11
Standard de cryptographie à clé publique.
PKCS#11 est une API spécifiée par RSA Labs qui définit un jeu de fonctions cryptographiques utilisables par les applications locales. Un module logiciel qui offre des fonctions PKCS#11 se nomme CRYPTOKI. PKCS#11.

CRYPTOLIB-CPS est le nom donné à un composant logiciel qui sait répondre à ces trois langages en utilisant la carte CPS.
Ce composant présente donc les trois interfaces :

- La bibliothèque CryptoAPI : CSP-CPS (environnements Windows).
- Le Tokend CDSA : GIP-CPS.tokend (environnements Macintosh).
- La bibliothèque PKCS#11 : PKCS#11-CPS (environnements Windows, MacOSX et Linux).

[1] Signature = garantie d'intégrité du message et d'authentification de son signataire (non répudiation).
[2] Authentification = garantie sur l'identité de l'émetteur.
[3] Dans le détail, il faudrait ajouter les Bi-Clés RSA et les fonctions cryptographiques RSA…

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

En complément, CRYPTOLIB-CPS s'appuie sur deux autres composants logiciels de gestion de la carte CPS et des lecteurs que nous nommerons :

- Composant API-CPS de gestion de la carte CPS dans un lecteur.
- Composant GALSS de gestion des lecteurs.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.2. ARCHITECTURE DES COMPOSANTS CRYPTOLIB-CPS, API-CPS ET GALSS

Ces trois composants, **CRYPTOLIB-CPS** (constitué des trois bibliothèques **CSP-CPS**, **GIP-CPS.tokend**, et **PKCS#11-CPS**), **API-CPS** et **GALSS** s'articulent suivant ce schéma de principe :

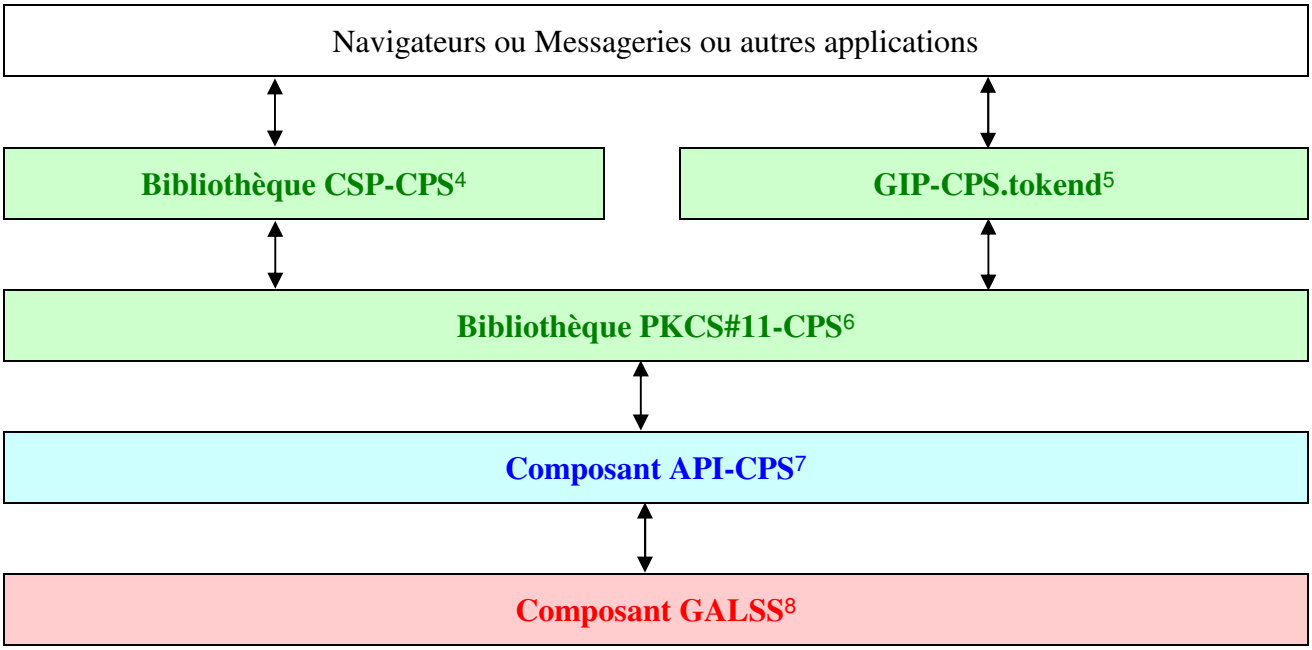


Figure 1 Architecture des composants CRYPTOLIB-CPS, API-CPS et GALSS

[4] La bibliothèque CSP-CPS n'existe que pour les OS Windows.
[5] La bibliothèque GIP-CPS.tokend n'existe que pour les OS Macintosh.
[6] La bibliothèque PKCS#11-CPS est implémentée pour les trois OS : Windows, Mac-OSX et Linux.
[7] Ce composant API-CPS est aussi utilisé par les applications à accès CPS (agent RSS, lecture Vitale, OSM, etc…)
[8] Ce composant GALSS est aussi utilisé par les applications de gestion des FSE (Sesam-Vitale)

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.3. WINDOWS : LE PROGRAMME CCM ASSOCIE A LA BIBLIOTHEQUE CSP-CPS

Si les deux bibliothèques CSP-CPS et PKCS#11-CPS offrent les mêmes fonctionnalités, leurs modes de fonctionnement diffèrent.
Chacun des deux modes induit une logique particulière de gestion des certificats X.509 situés dans la carte CPS.

Schématiquement, ces logiques sont :

- La bibliothèque PKCS#11-CPS renvoie ses certificats X.509 aux applications quand celles-ci la sollicitent.
  C'est donc à ce moment que la bibliothèque PKCS#11-CPS va rechercher les certificats X.509 dans la carte CPS.
- La bibliothèque CSP-CPS doit remonter ses certificats X.509 vers les applications (en fait, dans le magasin des certificats) pour que celles-ci la sollicitent…
  La bibliothèque CSP-CPS doit donc régulièrement rechercher les certificats X.509 dans la carte CPS (ou tout au moins s'assurer de la présence de la carte CPS dans le lecteur et qu'elle n'a pas été changée par une autre).

Cette fonction de surveillance de la présence d'une carte CPS dans le lecteur pour la bibliothèque CSP-CPS est assurée par un utilitaire, noté CCM [9] qui fonctionne en tâche de fond sur le poste Windows.

L'activité de CCM est matérialisée par la présence sur la barre des taches d'une icône spécifique :

Cadre vert : une carte CPS est présente dans le lecteur.
Ses certificats X.509 ont été recopiés dans le magasin Microsoft.

Cadre rouge et flèche orange : la carte CPS est en cours de lecture (état transitoire).
Les certificats sont en cours de copie dans le magasin Microsoft.

Cadre rouge et croix rouge : pas (ou plus) de carte CPS présente dans le lecteur.
Les certificats ont été effacés du magasin.

Cadre rouge, et point d'exclamation blanc sur triangle rouge : problème dans la configuration du poste empêchant l'accès au lecteur de cartes.

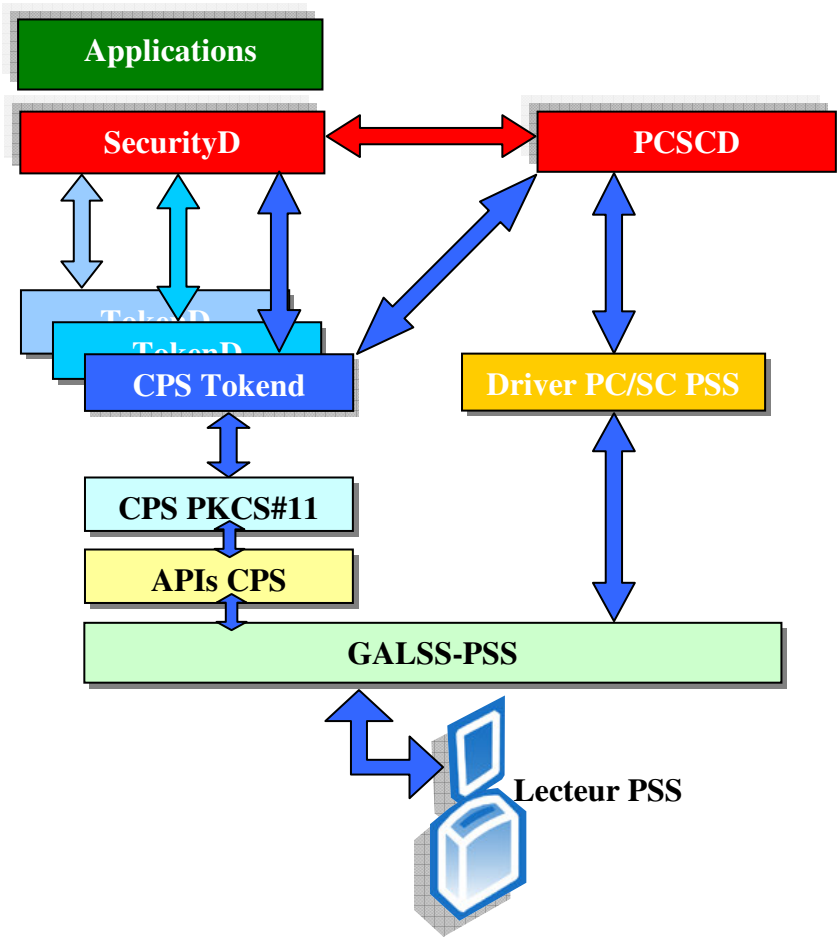
[9] Comme pour la bibliothèque CSP-CPS, ce CCM n'existe que pour les OS Windows.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.4. MACINTOSH : SPECIFICITES DE L'ARCHITECTURE CDSA / TOKEND

CDSA (Common Data Security Architecture) est un standard d'architecture de sécurité conçu par Intel et implémenté par Apple dans son système d'exploitation Mac OS-X.

Le cœur de CDSA est le module « serveur de sécurité » (SecurityD), qui s'appuie à la fois sur le protocole PC/SC (démon PCSCD) pour la gestion des lecteurs, et sur des modules appelés Tokend fournis par chaque organisme émetteur de cartes à puces pour la gestion de celles-ci :



Le serveur de sécurité, avec l'aide du gestionnaire de ressources PC/SC, détecte l'insertion d'une carte dans un lecteur. A ce moment là, le serveur de sécurité interroge les différents Tokend existant afin d'identifier celui qui gère cette carte. Le Tokend identifié et chargé, il est en mesure d'effectuer des opérations cryptographiques et de récupérer des objets (certificats, clés publiques…), à travers la carte.

Certaines applications Macintosh (ex : le navigateur Safari) se basent sur cette architecture et ne connaissent que celle-ci.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Les bibliothèques cryptographiques de l'ASIP Santé doivent donc s'intégrer dans CDSA pour que ces applications soient capables de fonctionner avec la carte CPS. Pour cela, l'ASIP fournit 2 composants :

- le **CPS Tokend** : module au standard Tokend d'Apple, qui permet de s'interfacer dans CDSA afin d'offrir le support de la carte CPS comme module cryptographique. Le Tokend est fondé sur l'architecture PC/SC pour la détection des cartes CPS et sur le module CPS PKCS#11 pour réaliser les opérations cryptographiques.

Avec un lecteur purement PC/SC, le module CPS Tokend est suffisant pour fonctionner. Mais puisque l'architecture d'un Tokend est basée sur ce seul protocole de communication, il est également nécessaire de fournir un driver PC/SC afin de pouvoir utiliser les lecteurs de type PSS (lecteurs série : bifente S-V et monofente NF-CPS) en plus des lecteurs PC/SC, et pouvoir ainsi couvrir la totalité des lecteurs susceptibles d'utiliser la carte CPS :

- le **driver PC/SC PSS** : c'est un driver simplifié qui permet d'intégrer les lecteurs PSS dans l'architecture PC/SC, au niveau du démon PCSCD. Il permet de détecter la présence d'une carte CPS dans les lecteurs de type RS232 (Série), en utilisant la couche GALSS-PSS. Son rôle est donc de prendre en charge les lecteurs de type PSS, qui pourront ainsi fonctionner dans l'environnement CDSA.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.5. LES CERTIFICATS X.509 DE LA CARTE CPS

Un certificat X.509 est un message (binaire) électronique, écrit suivant une syntaxe définie par la norme X.509, et signé par une autorité pour en garantir l'intégrité et la véracité de ses informations.

Les informations principales certifiées portent sur :

- L'identification de l'autorité ou émetteur, qui a signé ce certificat.
- Les dates de début et de fin de validité du certificat.
- L'identification du sujet ou objet, pour qui a été délivré ce certificat.
- La clé publique RSA [10].

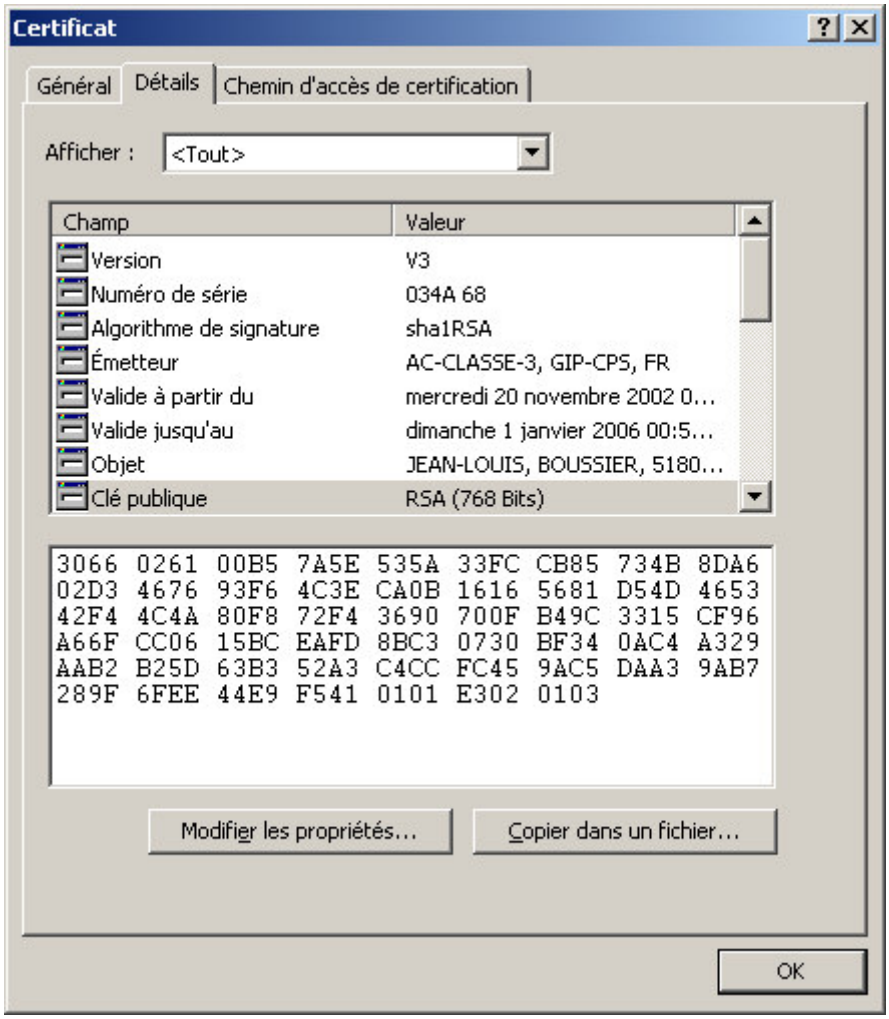


Figure 2 Exemple d'un certificat X.509 d'authentification d'une CPS2bis (CPA)

[10] L'algorithme cryptographique RSA utilise une clé en deux parties (bi-clé) : l'une est publique (diffusée dans le certificat X.509) et l'autre est privée (gardée secrète dans un coffre-fort logiciel ou dans une carte comme la CPS).
Il existe deux certificats X.509 (donc deux bi-clés) dans une CPS : l'un d'authentification et l'autre de signature.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.6. CHAINES DE CONFIANCE DES CERTIFICATS X.509 DE LA CARTE CPS

Si un certificat X.509 est signé par une autorité, celle-ci a elle-même un certificat, lui aussi signé par une autorité, et ainsi de suite jusqu'à rencontrer en tête de chaîne un certificat auto-signé (dit Racine ou Root) pour lequel ce sera bel et bien à l'utilisateur de manifester explicitement sa confiance.
Dans le cas de la carte CPS, les certificats racines sont publiés sur le site http://www.gip-cps.fr[11].
Toutes ces informations peuvent être vérifiées avant d'accorder sa confiance à ces certificats.

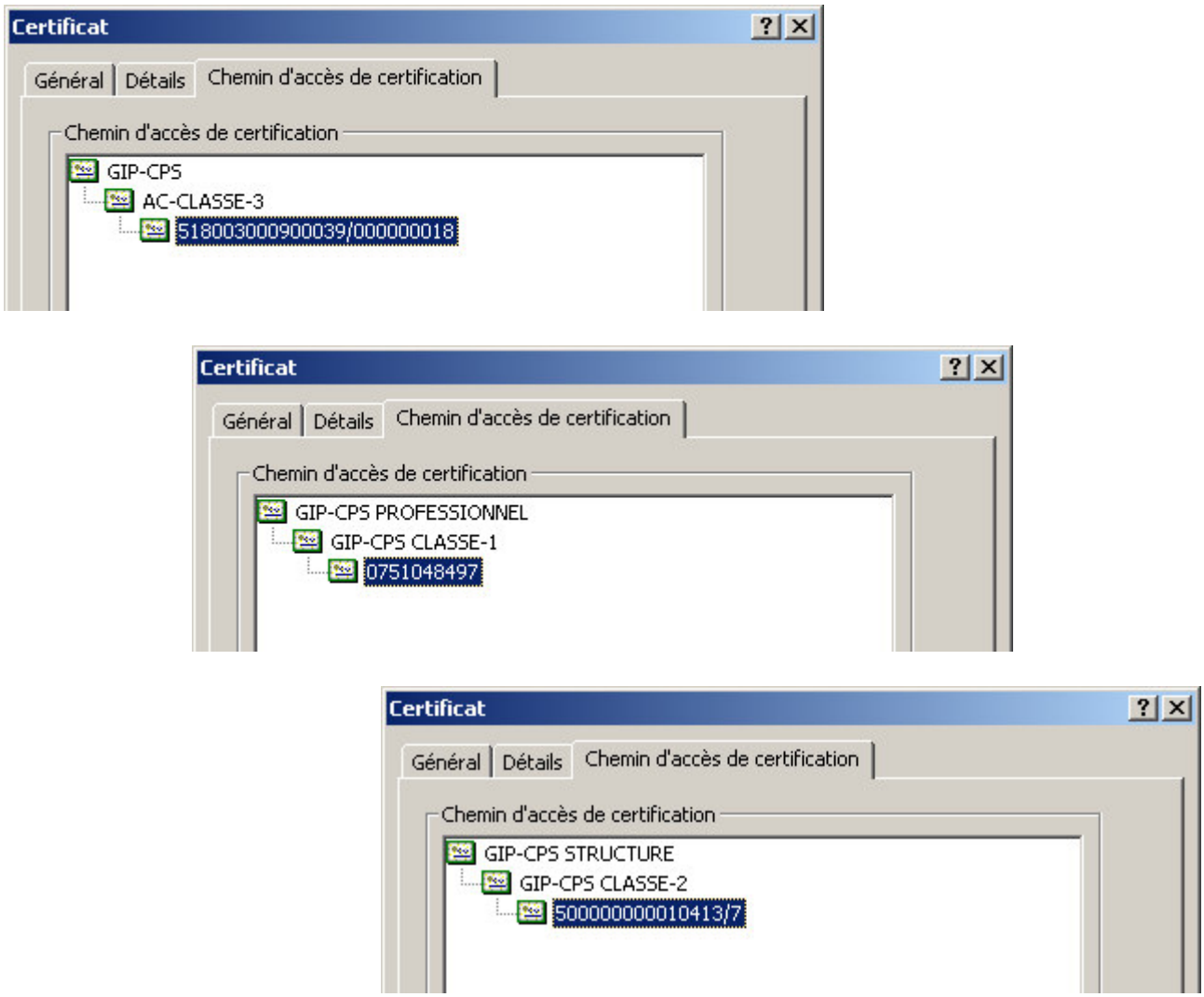


Figure 3 Exemples de chaînes de confiance de CPS

a) d'une CPS2bis (CPA)

b) d'une CPS2ter (CPS et CPF)

c) d'une CPS2ter (CDE)

[11] Ce site WEB est lui-même authentifié afin de garantir l'exactitude des informations publiées.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

2.7. LA LOGIQUE DU PROGRAMME D'INSTALLATION (CAHIER DES CHARGES)

Un module « chapeau » effectue tous les contrôles de faisabilité de l'installation, et les éventuelles saisies opérateur et construction du fichier de configuration du lecteur (GALSS.INI).
Il installe les chaînes de confiance de l'IGC CPS (pour les environnements Mac et Windows).
Il enchaîne les installations des trois composants GALSS, API-CPS et CRYPTOLIB-CPS.
Le setup du GALSS ne s'effectue que pour les configurations nouvelles ou modifiées.
En fin d'installation (Windows), la machine est redémarrée automatiquement pour enchaîner des tests de bon fonctionnement de l'ensemble.

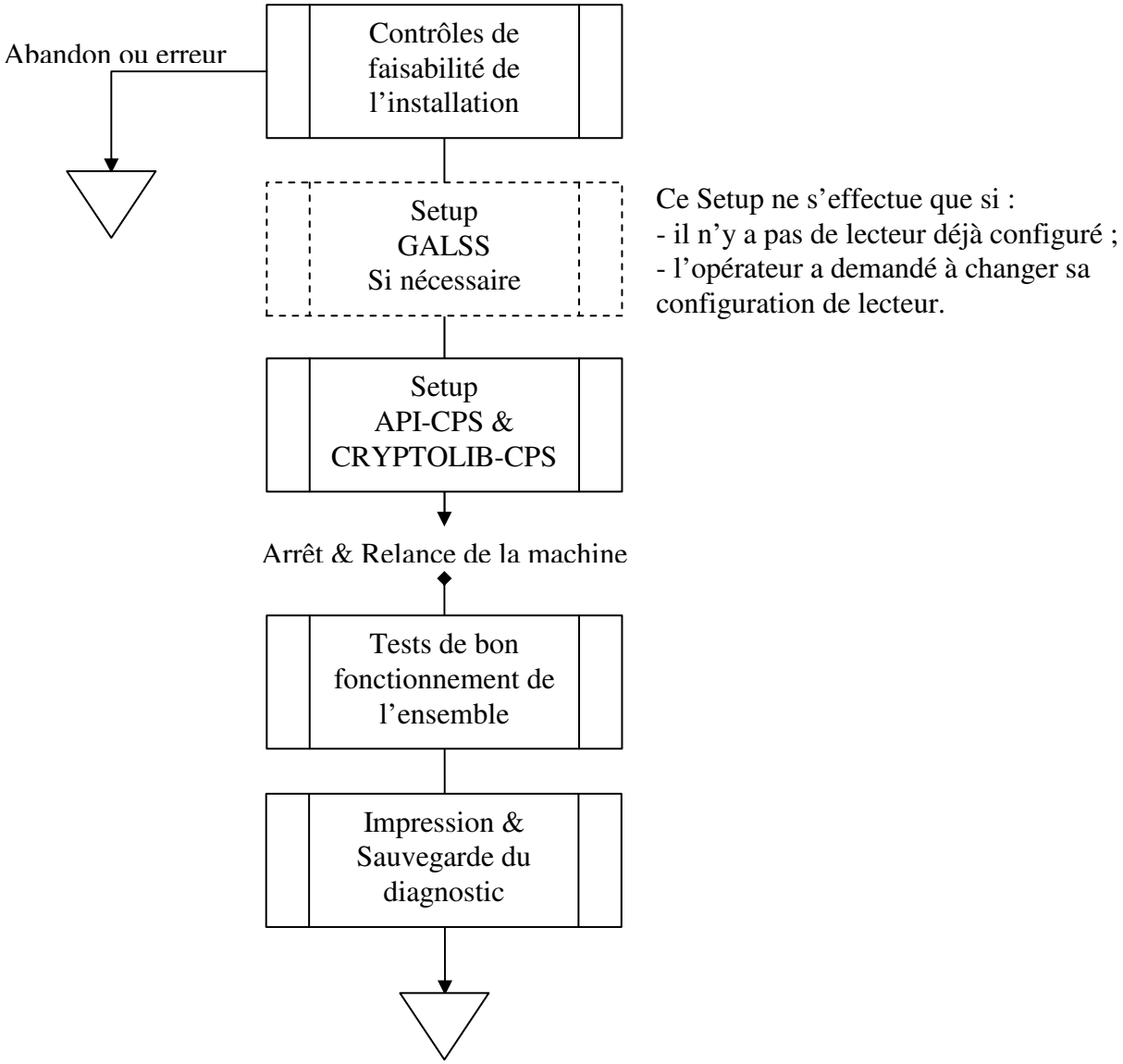

Abandon ou erreur
Contrôles de faisabilité de l'installation
Setup GALSS Si nécessaire
Ce Setup ne s'effectue que si :
- il n'y a pas de lecteur déjà configuré ;
- l'opérateur a demandé à changer sa configuration de lecteur.
Setup API-CPS & CRYPTOLIB-CPS
Arrêt & Relance de la machine
Tests de bon fonctionnement de l'ensemble
Impression & Sauvegarde du diagnostic

Figure 4 Organigramme de principe de l'installation

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

3. GUIDE D'INSTALLATION DE CRYPTOLIB

Nous remercions l'utilisateur de suivre scrupuleusement ce guide…

3.1. LES PRE REQUIS AVANT TOUTE INSTALLATION

1. Le système d'exploitation (OS) de votre machine doit être l'un des trois :
   - Windows (XP SP3, Server 2003, Server 2008, Vista, Seven).
   - Mac OS X (à partir de la version 10.4) [12].
   - Linux (Noyau 2.4 ou 2.6).

   Et vous devez avoir les droits d'Administrateur sur cet OS.

   Sinon, abandonnez l'installation !

   Attention : Sous Windows Vista ou Seven, la version minimum du setup Cryptolib à installer est la 3.06, incluant la version 3.26 du composant GALSS.

   Attention : dans le cas d'une configuration de type TSE/Citrix (architecture client/serveur), la version minimale du composant GALSS devra être la 3.22.
2. A votre machine est connecté, et en état de bon fonctionnement[13], au moins un de ces trois types de lecteurs :
   - Lecteur bi-fente « sesam-vitale » connecté sur un port COM. L'adresse physique de ce type de lecteur doit être configurée sur la valeur constructeur par défaut, c'est-à-dire **2** (cf. la documentation de votre lecteur pour la configuration de ce paramètre).
   - Lecteur mono-fente « NF CPS » connecté sur un port COM. L'adresse physique de ce type de lecteur doit être configurée sur la valeur constructeur par défaut, c'est-à-dire **0** (cf. la documentation de votre lecteur pour la configuration de ce paramètre).
   - Lecteur mono-fente « PC/SC » quelque soit son type de connexion.

   Sinon, abandonnez l'installation, installez un de ces lecteurs et reprenez cette installation…

   Attention pour le lecteur de type PC/SC : il faut qu'il soit physiquement connecté et que son pilote (driver) PC/SC ait été aussi installé avec succès (à partir d'une disquette ou CD fourni par son fournisseur). Il est également conseillé d'avoir effectué un arrêt et redémarrage de la machine pour une bonne prise en compte du lecteur PC/SC.
3. Vous disposez de votre carte CPS dans ce lecteur.

   Sinon, abandonnez l'installation que vous reprendrez avec votre CPS…
4. Vous êtes en condition d'accepter un redémarrage de votre machine :
   - Vous avez fermé tout document, fichier ou application « sensibles ».
   - Vous avez fermé toute application ou utilitaire à accès CPS.

[12] La prise en charge des lecteurs série (i.e. lecteurs bifente) avec le navigateur Safari sous Léopard (OS X 10.5) n'est possible qu'à partir de la release 10.5.6 de cet OS, avec une installation Cryptolib V03.12 minimum.

[13] Ce pré requis est implicite si vous utilisez déjà une/des applications sur carte CPS (FSE, lecture Vitale, OSM…)

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Attention : certains utilitaires (agent RSS, OSM, etc…) sont difficilement visibles et/ou nécessitent l'arrêt au préalable de toute messagerie.

- Dans le doute, fermez vos navigateurs et messageries.

Sinon, effectuez ces fermetures avant de poursuivre l'installation…

5. Cas particulier : si vous aviez déjà effectué précédemment une installation de CRYPTOLIB-CPS sur votre machine Windows, commencez par « Supprimer » cette installation !

   Exemple, par « Démarrer » ; « Paramètres » ; « Panneau de configuration » ; « Ajout/Suppression de programmes » ; « Cryptolib CPS » ; « Modifier/Supprimer » ; « Désinstallation complète »…

3.2. INSTALLATION

Rappel d'un pré requis : vous êtes en condition d'accepter un redémarrage de votre machine :

- Vous avez fermé tous vos documents, fichiers ou applications « sensibles »
- Vous avez fermé toute application ou utilitaire à accès CPS

6. Insérez votre CPS dans votre lecteur et ouvrez le CD ou le package d'installation de CRYPTOLIB-CPS.
   - Windows : le programme « **InstallationWindows.exe** » doit démarrer (sinon, lancez-le)
   - Linux : exécutez, en mode console, le script « **InstallationLinux.sh** »
   - Mac OS X : exécutez le programme « **Installation MacOSX** »

7. L'installation de CRYPTOLIB-CPS s'effectue de façon standard.
   - Validez, après lecture, toutes les demandes. Sous Windows, l'installation se termine par une demande de relancer la machine.
   - Cas particulier si l'installation vous demande de choisir un lecteur :
     Ce cas se produit sur une machine sur laquelle vous n'avez jamais exploité de carte CPS dans un lecteur. L'installation vous demande donc de choisir le lecteur qu'elle doit tester et configurer.
     Ce cas pourra se reproduire aussi sur cette machine lorsque vous referez cette installation, vous pourrez alors changer le lecteur qu'elle doit tester et configurer.

8. Laissez en place votre CPS et le CD d'installation le cas échéant, et acceptez le redémarrage de la machine.

   << Redémarrage de la machine… >>

9. En fin d'installation, un test de bon fonctionnement est exécuté. Son exécution est automatique sous Windows, dans les autres environnements c'est l'opérateur qui doit le lancer manuellement en exécutant de nouveau le programme d'installation (cf. point 6 ci-dessus). A la fin de ce test un diagnostic est affiché, que vous pouvez imprimer et sauvegarder. Vous pouvez maintenant enlever le CD ou supprimer le package logiciel d'installation.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

10. Remarque concernant l'environnement Windows : si la personne qui va utiliser Cryptolib sur ce poste ne possède pas les droits d'Administrateur, l'opérateur doit s'assurer que les répertoires *Coffre* et *Traces* du dossier *"\Program Files\Cryptolib CPS"* possèdent bien les droits de lecture et d'écriture pour cet utilisateur.

Si l'installation s'est bien terminée, les composants logiciels sont maintenant disponibles sur votre machine.

En environnement Windows, vous devez trouver (la carte étant toujours présente dans le lecteur) l'icône du programme CCM (couleur jaune bordée de vert), comme indiqué sur la figure ci-dessous :

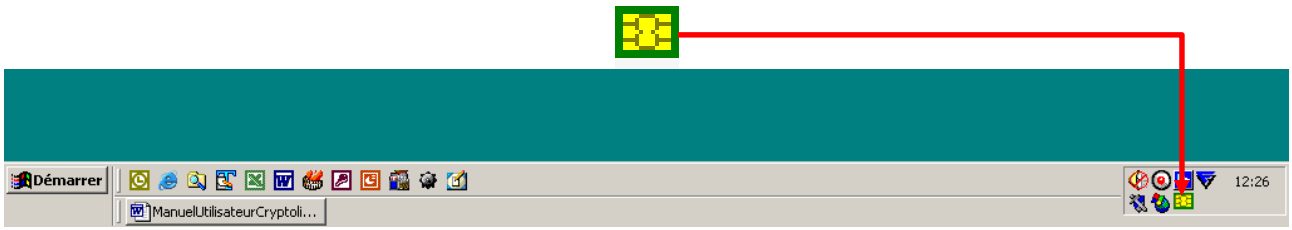


Figure 5 Exemple de barre des tâches sous Windows avec CCM

Pour les autres environnements Linux et Mac, aucun élément visible de ce type n'est à contrôler…
Il reste cependant à vérifier que leur utilisation rend bien le service attendu.

Vous allez effectuer ce test à partir de votre navigateur usuel (et le plus récent possible) tel que décrit dans la partie guide d'utilisation de ce manuel : par une connexion en HTTPS.

3.3. DESINSTALLATION

Pour la désinstallation, exécutez votre package d'installation de CRYPTOLIB-CPS de la même manière que lors de la phase d'installation. Il vous sera alors demandé de confirmer la désinstallation.

En revanche, ce setup ne permet pas :

- De désinstaller le logiciel GALSS, les API CPS ou les bibliothèques Cryptolib : ceci afin de ne pas risquer de détériorer la configuration existante du poste de travail.
- De modifier une installation défaillante si elle n'a pas été réalisée déjà par cette même procédure. Il faudra alors vous adresser au prestataire informatique qui a configuré ce poste.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4. GUIDE D'UTILISATION DE CRYPTOLIB

Les trois exemples qui suivent montrent une connexion HTTPS sécurisée par CPS sur un site de test de l'ASIP Santé (testssl.gip-cps.fr).

Ce serveur demande au poste client de s'authentifier par un certificat X.509 explicitement reconnu comme appartenant à l'Infrastructure de Gestion des Clés (IGC) CPS.

La connexion HTTPS se fera par un navigateur :

1. **Internet Explorer** montre une utilisation de la bibliothèque CSP-CPS de CRYPTOLIB-CPS

   Si cette connexion réussit, alors toute autre connexion sécurisée par CPS sur d'autres sites doit aussi fonctionner ; ainsi que toute application développée sur ce standard Microsoft CryptoAPI.

2. **Safari** montre une utilisation de la bibliothèque GIP-CPS.tokend de CRYPTOLIB-CPS

   Si cette connexion réussit, alors toute autre connexion sécurisée par CPS sur d'autres sites doit aussi fonctionner ; ainsi que toute application développée sur ce standard Apple CDSA.

3. **Mozilla FireFox** montre une utilisation de la bibliothèque PKCS#11-CPS de CRYPTOLIB-CPS

   Si cette connexion réussit, alors toute autre connexion sécurisée par CPS sur d'autres sites doit aussi fonctionner ; ainsi que toute application développée sur ce standard RSA PKCS#11.

Le premier et le troisième exemple sont effectués sur l'environnement **Windows**. Mais celui de **Mozilla FireFox** peut être transposé sur les deux autres environnements **Linux** et **Mac OS X** car ce navigateur existe pour les trois environnements. Le deuxième exemple est lui effectué sur l'environnement Mac OS X, car il concerne le navigateur **Safari** livré avec cet OS.

Remarque : la terminologie suivante est utilisée pour les dossiers système de Windows :
%WINDIR% correspond au dossier C:\Windows
%WINSYS% correspond au dossier C:\Windows\System32

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.1. CONNEXION HTTPS PAR INTERNET EXPLORER (WINDOWS)

4.1.1. Contrôles sur l'utilitaire CCM

Avant de travailler avec le navigateur, il faut s'assurer que l'utilitaire CCM a bien détecté la carte CPS dans le lecteur comme décrit sur la Figure 5.

Cet utilitaire CCM assure la synchronisation entre le magasin Microsoft des certificats utilisateur et la carte CPS. Ce programme n'existe que sous Windows.

Pour visualiser ce magasin de certificats, lancez Internet Explorer, sélectionnez le menu « Outils », puis « Options internet… », dans l'onglet « Contenu » cliquez sur le bouton « Certificats ». La fenêtre qui apparaît affiche le magasin des certificats personnels de l'utilisateur.

- Si une carte CPS est introduite dans un lecteur connecté sur le poste, le CCM permet l'ajout des certificats associés à cette carte au magasin de certificats personnel.
- Si une carte CPS est retirée d'un lecteur connecté sur le poste, le CCM permet le retrait des certificats associés à cette carte du magasin de certificats personnels.

Ce processus est indispensable si vous voulez utiliser votre carte CPS avec Internet Explorer, Outlook, ou Outlook Express.

Lors de l'installation, le programme CCM.exe est ajouté à la liste des programmes devant être lancé au démarrage du poste.

Le programme est également présent dans le menu « Démarrer » ; « Programmes » ; « Cryptolib CPS », sous le nom « Gestionnaire de certificats CPS ».

Au lancement, ce programme signale sa présence par un icône reflétant l'état du lecteur de carte CPS.

L'icône du programme peut avoir quatre états différents :

1	Etat représentant l'absence de carte CPS dans un lecteur.	
2	Etat transitoire représentant la lecture en cours d'une carte CPS…	
3	Etat représentant la présence de la carte CPS dans un lecteur et de ses certificats dans le magasin de certificats de l'utilisateur.	
4	Etat représentant une erreur survenue lors du traitement (accès au lecteur, composants manquants…).	

C'est bien sûr l'état 3 qui est attendu !

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Le programme CCM est doté d'un menu contextuel (**« clic droit » sur l'icône**) permettant de le configurer ou d'obtenir des informations sur ce dernier. Les menus affichés sont les suivants :

1 - A propos de CCM… affiche les informations sur le programme CCM.

2 - Basculer en surveillance automatique de l'état du lecteur permet de détecter automatiquement le retrait (ou la présence) éventuel d'une carte CPS. Lorsque le basculement à lieu, le menu change et affiche *Basculer en surveillance manuelle de l'état du lecteur*.

- Basculer en surveillance manuelle de l'état du lecteur désactive la détection automatique du retrait éventuel (ou la présence) d'une carte CPS.

> **Afin de vérifier la présence ou l'absence d'une carte CPS dans le lecteur et donc de faire (ou ne plus faire) apparaître les certificats de la carte dans le magasin de certificats personnels, il faudra que l'utilisateur rafraîchisse explicitement l'état du lecteur via le menu correspondant**.

Lorsque le basculement a lieu, le menu change et affiche *Basculer en surveillance automatique de l'état du lecteur*.

3 - Rafraîchir l'état du lecteur est accessible uniquement en mode de surveillance manuelle.

4 - Lister l'état des lecteurs… Affiche l'état de tous les lecteurs présents et configurés sur le poste. Il est accessible uniquement si plusieurs lecteurs de cartes CPS sont présents sur le poste.

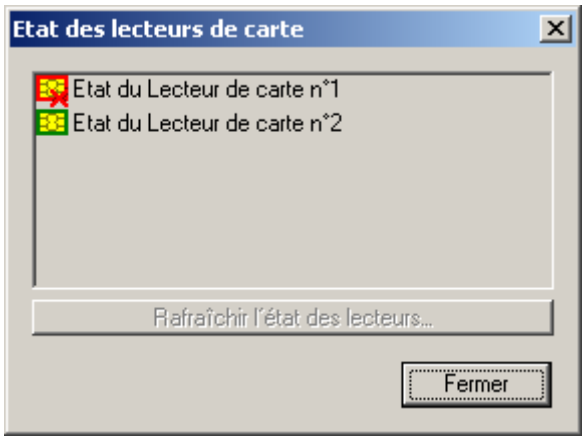


Figure 6 CCM : exemple d'état de deux lecteurs dont un avec une CPS

5 - Quitter permet de quitter le programme CCM

Lors de la première exécution du programme CCM, la surveillance **manuelle** de l'état du lecteur est activée par défaut.

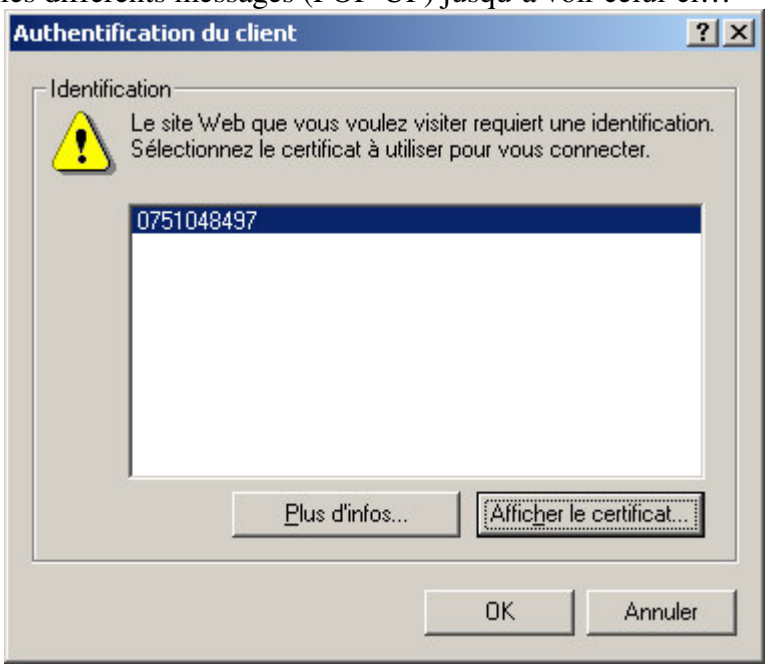
Le mode de surveillance (manuelle ou automatique) choisi est reconduit à chaque redémarrage de la machine.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.1.2. Connexion HTTPS

Lancez Internet Explorer et saisissez dans la zone adresse : https://testssl.gip-cps.fr (ou http://testssl.gip-cps.fr puis cliquez sur la proposition de https://testssl.gip-cps.fr)

Acceptez et validez les différents messages (POP-UP) jusqu'à voir celui-ci…



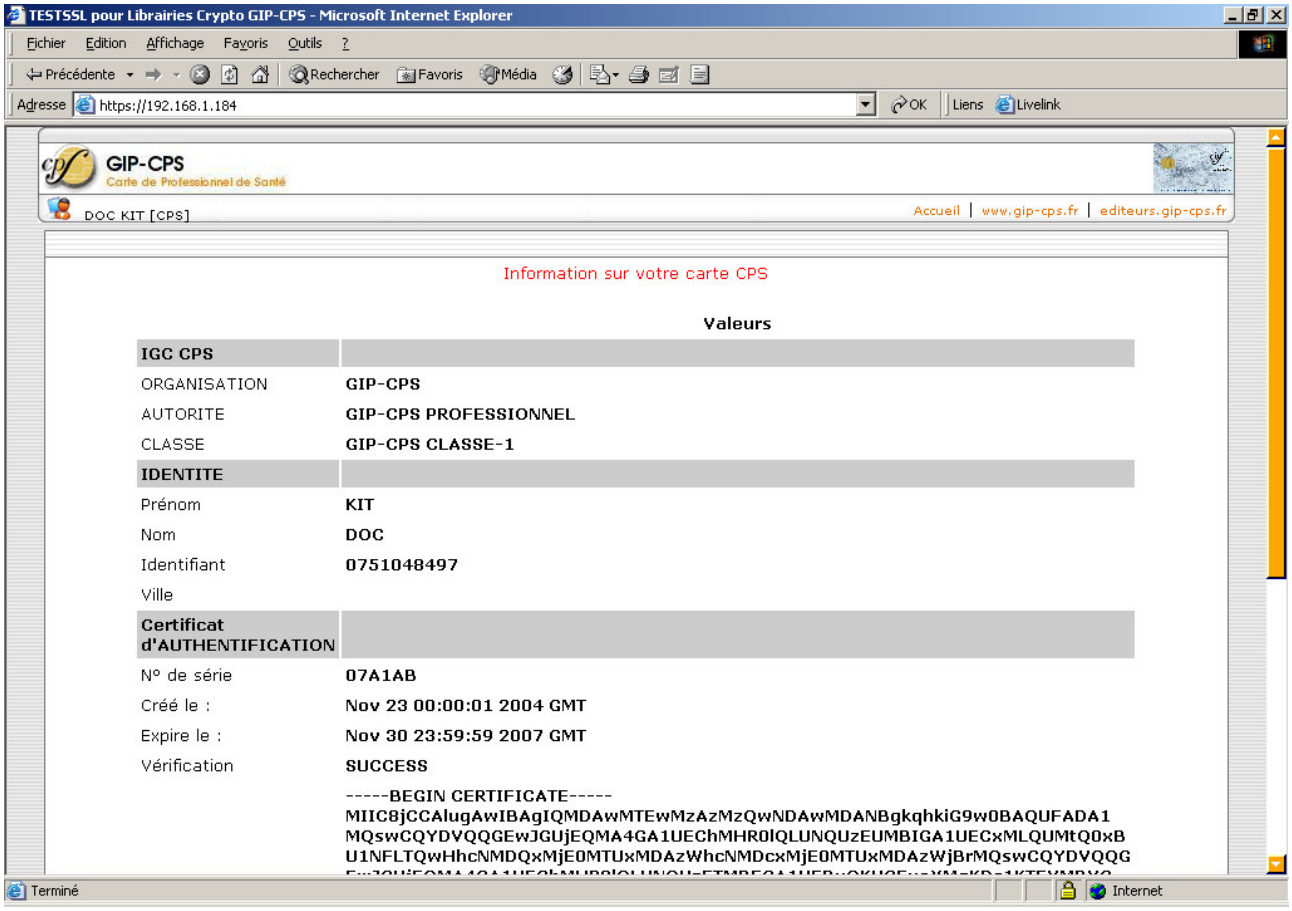
…qui correspond au certificat X.509 d'authentification de votre carte CPS (vous pouvez l'afficher). Validez le message.

Attention sur l'invite suivante :

Il vous est demandé de saisir les 4 chiffres du code porteur de la carte CPS.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Jusqu'au succès de l'authentification qui se manifeste par ce type de fenêtre d'accueil du serveur[14] :



[14] Cette recopie d'écran est donnée à titre indicatif. La page réelle affichée sur le site de test du GIP-CPS peut être différente.

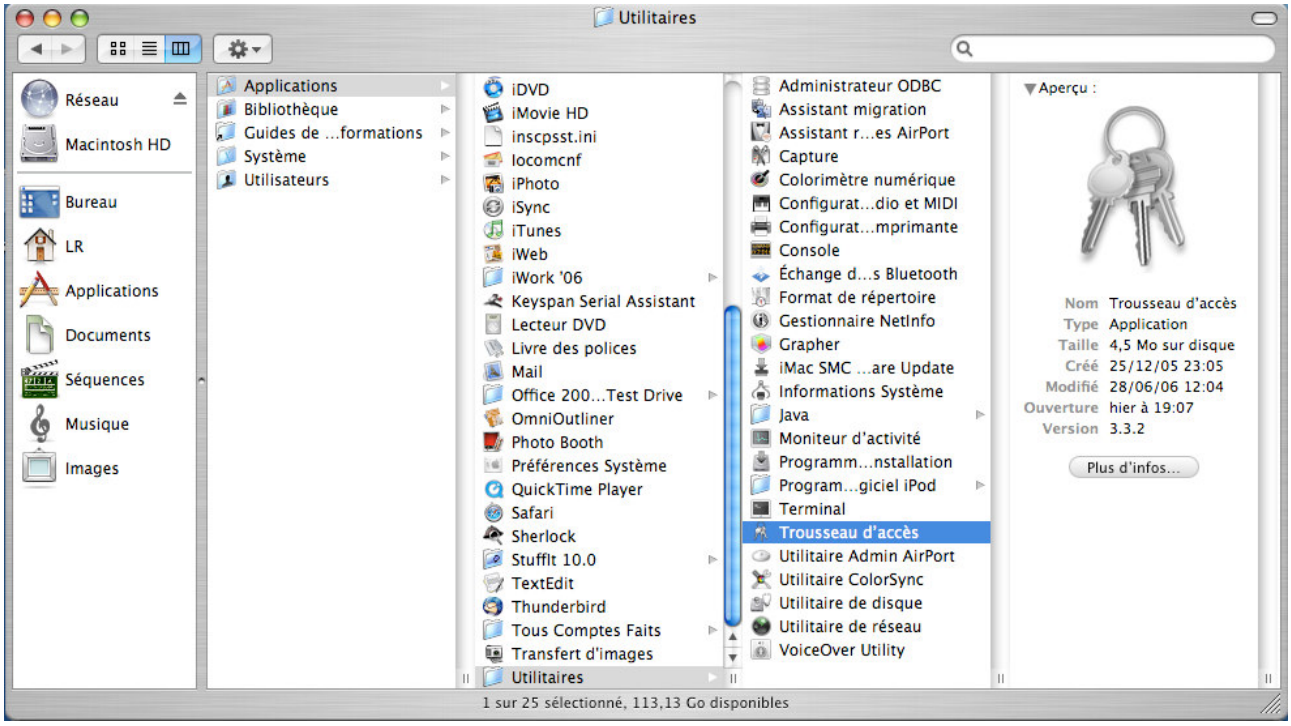
© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.2. CONNEXION HTTPS PAR SAFARI (MACINTOSH)

4.2.1. Contrôles visuels de l'installation

Une fois l'installation effectuée il est possible de vérifier le bon fonctionnement du Tokend CDSA (et donc de l'ensemble des éléments installés) à l'aide du programme de visualisation des clés et des certificats inclus dans l'OS.

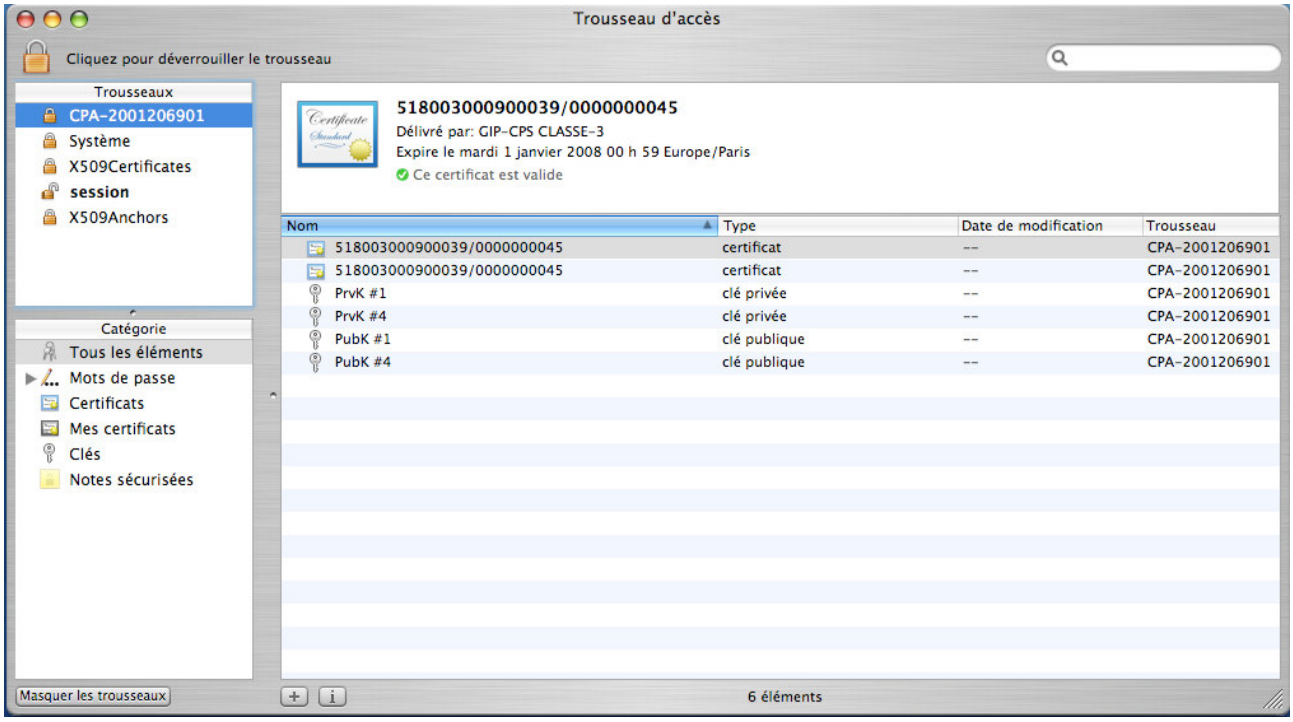
Insérez une carte CPS dans votre lecteur, puis lancez ce programme, nommé *Trousseau d'accès,* et qui se trouve dans le dossier */Applications/Utilitaires/* :



© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Une fois cette application lancée, vous pouvez voir la liste des « Trousseaux » au dessus de la zone « Catégorie ». Si cette liste n'est pas affichée, cliquez sur le bouton « Afficher les trousseaux » (en bas à gauche de la fenêtre).

Vérifiez alors que le nom de votre carte s'affiche bien dans cette liste, sous la forme CP*x-NuméroDeCarte*[15], ainsi que le montre l'exemple suivant :



La présence de ce trousseau indique la bonne installation et le bon fonctionnement de l'ensemble des composants de l'ASIP Santé : la carte a été lue correctement et elle est bien vue comme un Tokend par le système.

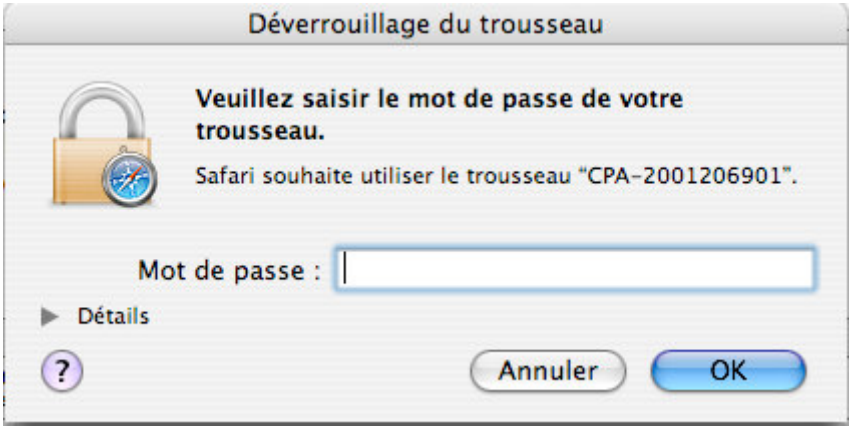
[15] NuméroDeCarte = numéro à 10 chiffres inscrit sous le patronyme sur le visuel de la carte.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.2.2. Connexion HTTPS

Lancez Safari et saisissez dans la zone adresse : https://testssl.gip-cps.fr (ou http://testssl.gip-cps.fr puis cliquez sur la proposition de https://testssl.gip-cps.fr).

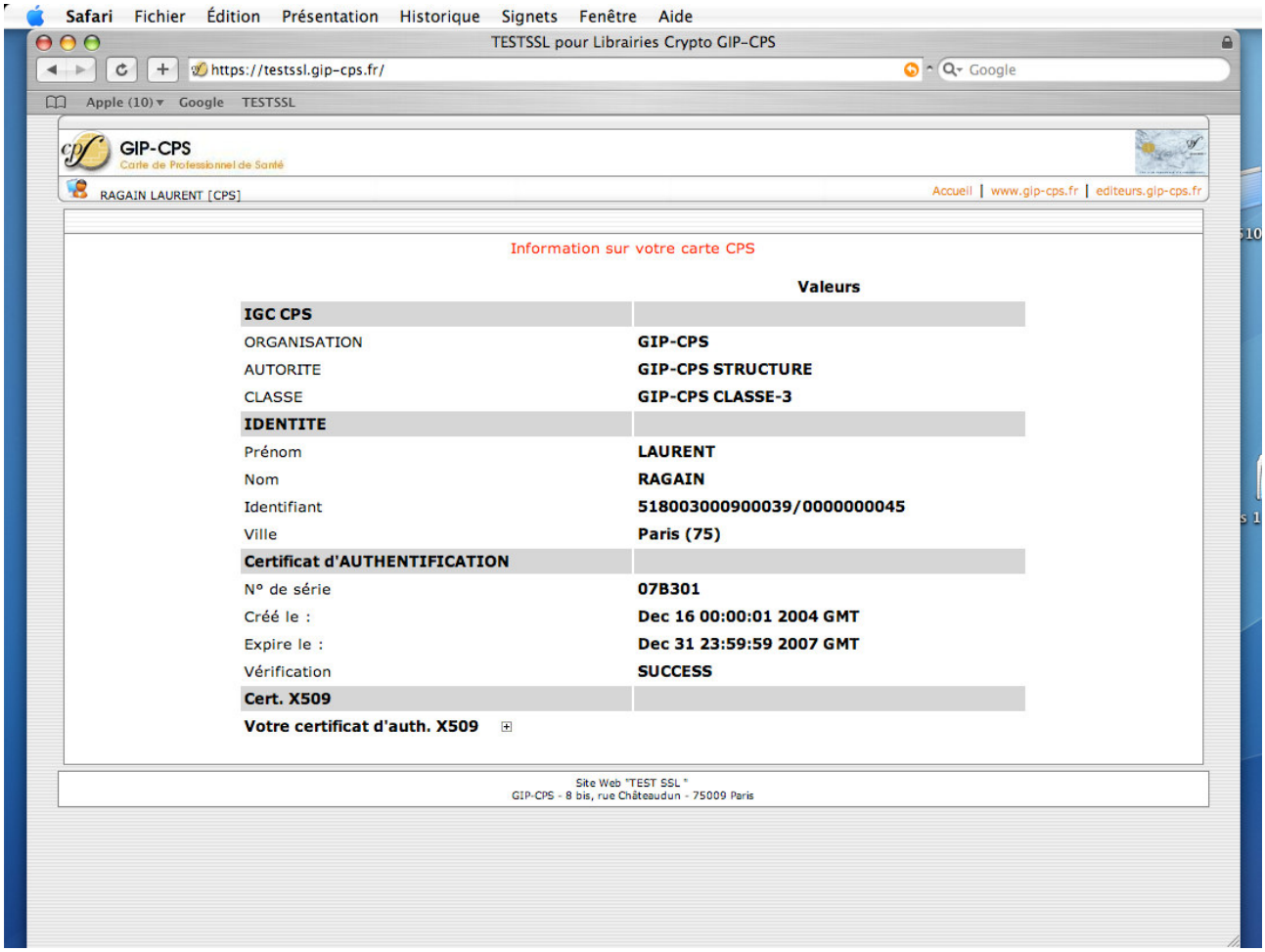
Attention sur l'invite suivante :



Il vous est demandé de saisir les 4 chiffres du code porteur de la carte CPS.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Jusqu'au succès de l'authentification qui se manifeste par ce type de fenêtre d'accueil du serveur[16] :



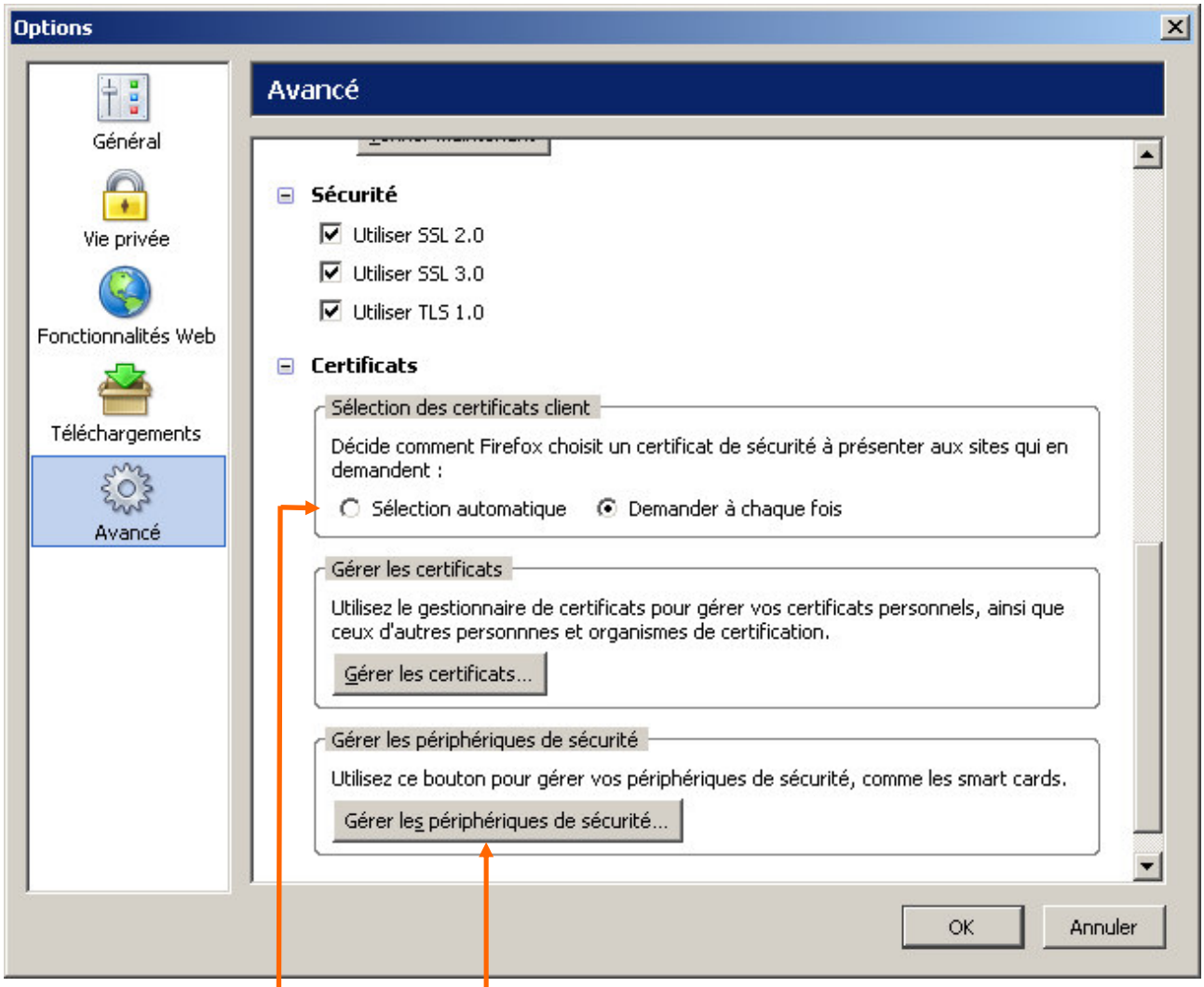
[16] Cette recopie d'écran est donnée à titre indicatif. La page réelle affichée sur le site de test du GIP-CPS peut être différente.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.3. CONNEXION HTTPS PAR MOZILLA FIREFOX (WINDOWS, LINUX, MAC-OSX)

4.3.1. Ajout du périphérique PKCS#11-CPS dans Firefox

Après avoir lancé le navigateur Firefox, il faut le paramétrer (dans menu : « **outils** » ; « **options** » ; « **Avancé** » ; éventuellement onglet « **Chiffrement** » selon votre version de Firefox) afin qu'il connaisse la bibliothèque CRYPTOLIB-CPS.

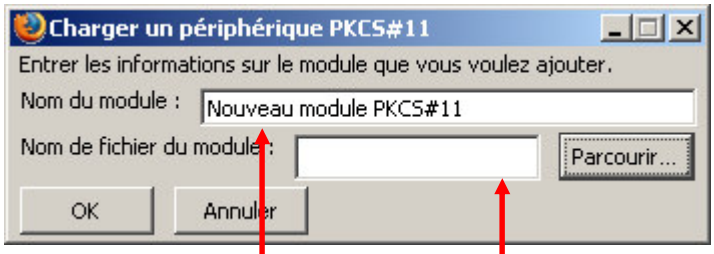

Options
Général
Vie privée
Fonctionnalités Web
Téléchargements
Avancé
Avancé
Sécurité
Utiliser SSL 2.0
Utiliser SSL 3.0
Utiliser TLS 1.0
Certificats
Sélection des certificats client
Décide comment Firefox choisit un certificat de sécurité à présenter aux sites qui en demandent :
Sélection automatique
Demander à chaque fois
Gérer les certificats
Utilisez le gestionnaire de certificats pour gérer vos certificats personnels, ainsi que ceux d'autres personnnes et organismes de certification.
Gérer les certificats...
Gérer les périphériques de sécurité
Utilisez ce bouton pour gérer vos périphériques de sécurité, comme les smart cards.
Gérer les périphériques de sécurité...
OK
Annuler

Cliquez sur « **Gérer les périphériques de sécurité**… » et demandez à « **charger** » un périphérique PKCS#11 …

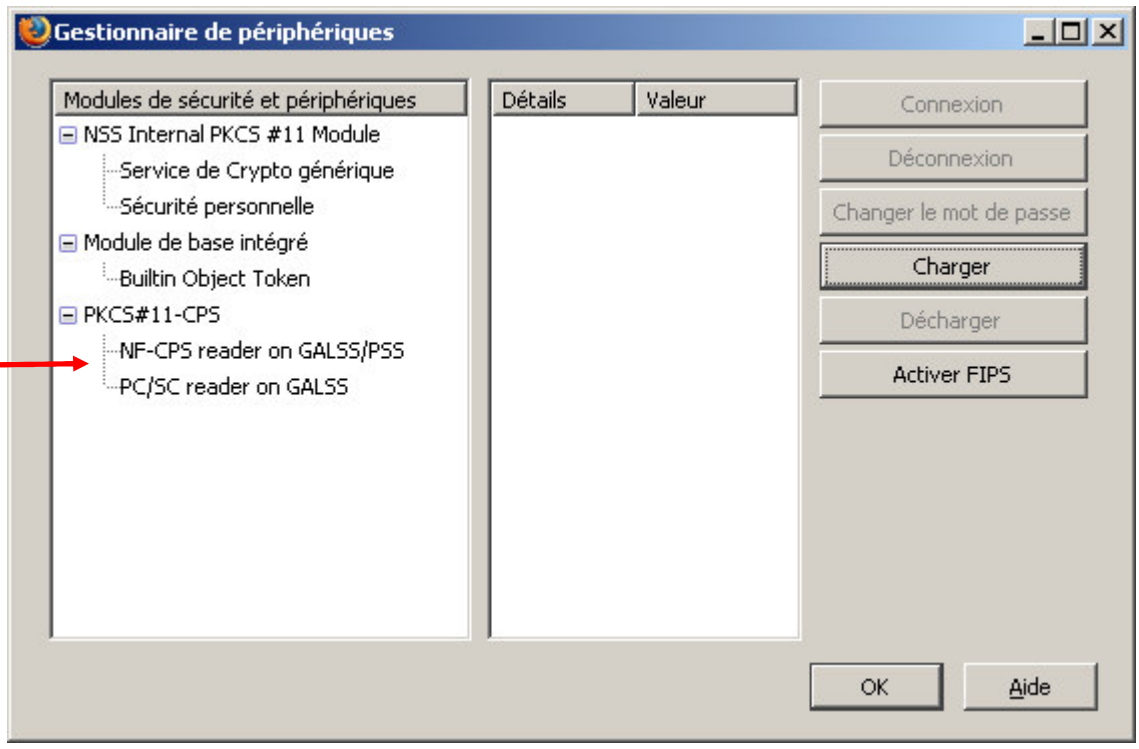
Attention : pour les versions 3.5 et supérieures de Firefox, conservez comme ici l'option par défaut « Demander à chaque fois ». Mais pour Firefox 3, choisissez l'option « Sélection automatique ».

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Entrez les informations sur le module à ajouter :



Entrez :
Nom du module : PKCS#11-CPS
Nom du fichier du module : C:\Windows\cps_pkcs11_w32.dll[17]
Et validez…



Remarque : vous devez alors voir le lecteur de CPS (ici 2 lecteurs ont été configurés).

Validez les fenêtres ouvertes jusqu'à fermer la fenêtre « options »… L'ajout est terminé, le test de la connexion peut se faire…

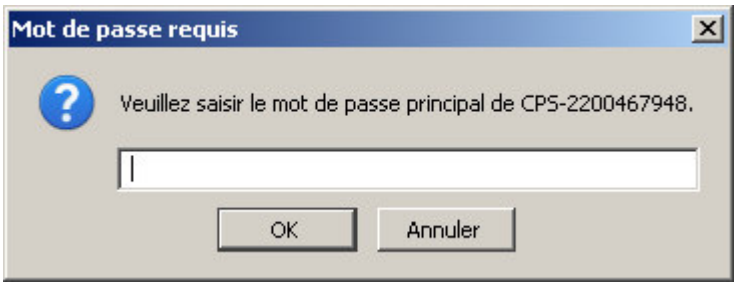
[17] Sous Linux : /usr/local/galss/libcps_pkcs11_lux.so
Sous Mac OSX : /usr/lib/libcps_pkcs11_osx.dylib

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4.3.2. Connexion HTTPS

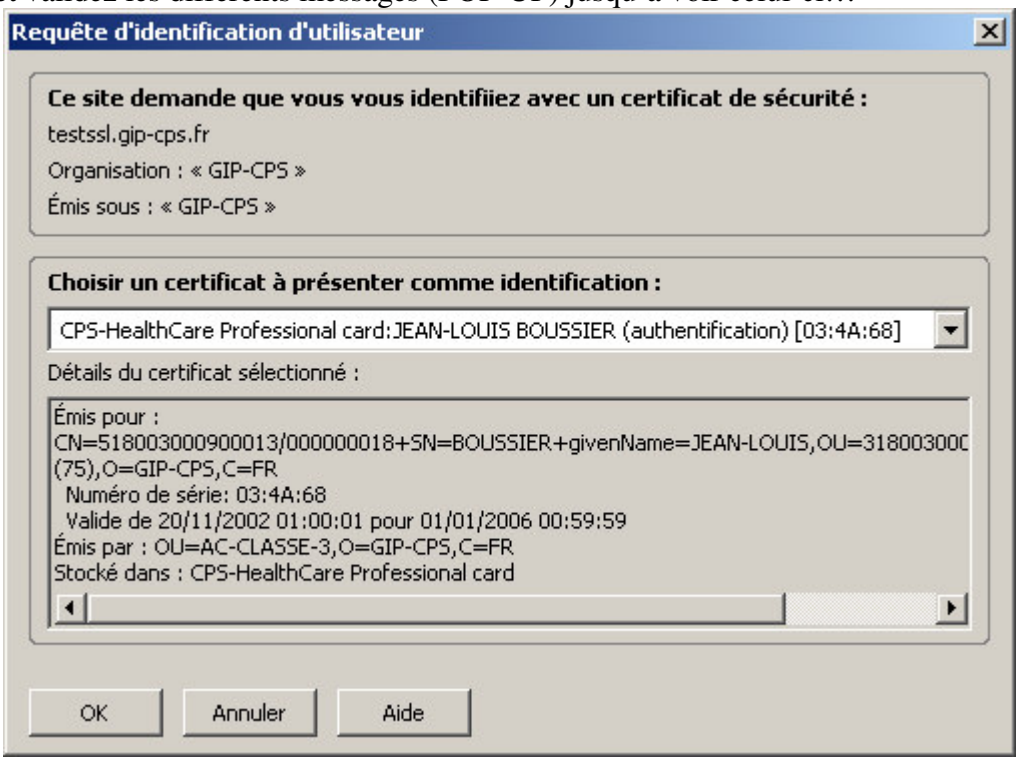
Vous pouvez maintenant saisir dans la zone adresse : https://testssl.gip-cps.fr (ou http://testssl.gip-cps.fr puis cliquez sur la proposition de https://testssl.gip-cps.fr).

Attention sur l'invite suivante :



Il vous est demandé de saisir les 4 chiffres du code porteur de la carte CPS.

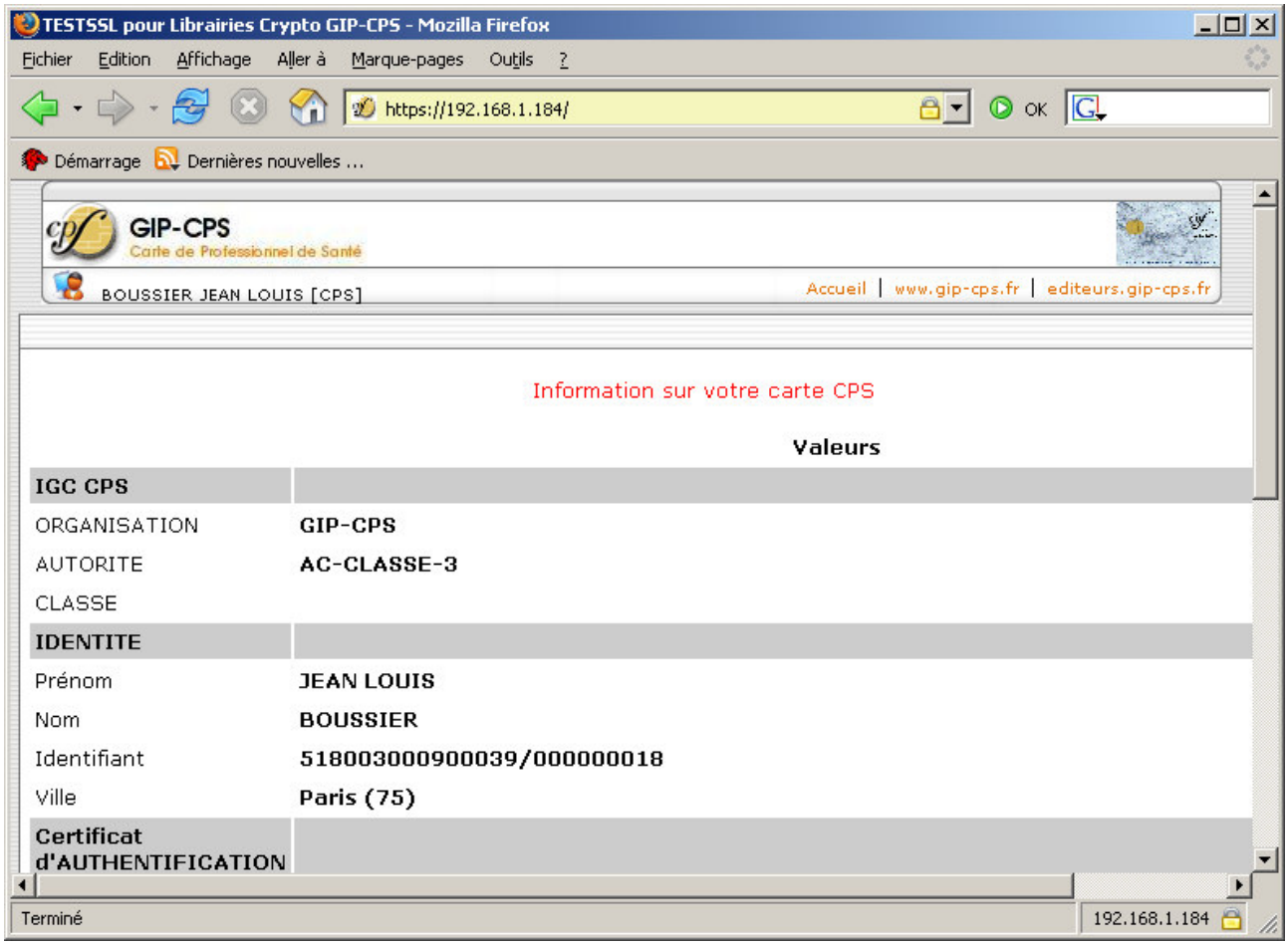
Acceptez et validez les différents messages (POP-UP) jusqu'à voir celui-ci…


Requête d'identification d'utilisateur
Ce site demande que vous vous identifiiez avec un certificat de sécurité :
testssl.gip-cps.fr
Organisation : « GIP-CPS »
Émis sous : « GIP-CPS »
Choisir un certificat à présenter comme identification :
CPS-HealthCare Professional card:JEAN-LOUIS BOUSSIER (authentification) [03:4A:68]
Détails du certificat sélectionné :
Émis pour :
CN=518003000900013/000000018+SN=BOUSSIER+givenName=JEAN-LOUIS,OU=318003000
(75),O=GIP-CPS,C=FR
Numéro de série: 03:4A:68
Valide de 20/11/2002 01:00:01 pour 01/01/2006 00:59:59
Émis par : OU=AC-CLASSE-3,O=GIP-CPS,C=FR
Stocké dans : CPS-HealthCare Professional card
OK
Annuler
Aide

…qui correspond au certificat X.509 d'authentification de votre carte CPS.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Jusqu'au succès de l'authentification qui se manifeste par ce type de fenêtre d'accueil du serveur[18] :



[18] Cette recopie d'écran est donnée à titre indicatif. La page réelle affichée sur le site de test du GIP-CPS peut être différente.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5. AIDES AUX DIAGNOSTICS

5.1. COMPTE RENDU DE FIN D'INSTALLATION

En fin d'installation, après l'arrêt et la relance de la machine, il vous est affiché un compte-rendu que vous pouvez imprimer et sauvegarder. En voici un extrait en exemple avec les points principaux à contrôler :

	Contrôlez :
Installation des composants CPS v02.00	02.00 minimum impératif
…	
Version du GALSS, … = 03.11	Peut être 02.xx
Version des APIs CPS = 05.03	05.03 minimum impératif
Version de la bibliothèque PKCS#11 = 01.07	01.07 minimum impératif
Version de la bibliothèque CSP = 01.21	01.21 minimum impératif
Version de l'utilitaire CCM = 02.01	02.01 minimum impératif
…	
Contrôle des versions des logiciels CPS = rc=0 (0000H) [OK.]	[OK.] impératif
Contrôle de conformité de la configuration = rc=0 (0000H) [OK.]	[OK.] impératif
…	
Etat de fonctionnement du lecteur de cartes CPS = rc=	Varie suivant l'état de la carte
Etat de fonctionnement des bibliothèques PKCS#11 = OK.	[OK.] impératif
Etat de fonctionnement des bibliothèques CSP = OK.	[OK.] impératif
…	
Contenu du fichier GALSS.INI	Fichier de configuration ;
…	Doit contenir cette ligne :
NomLAD=CPS[19]	
…	

D'autres lignes sont éditées qui pourront vous être demandées en cas d'appel pour maintenance.

Remarque : Sous Linux, le compte-rendu détaillé des tests est enregistré dans :
/root/INSTALL_CRYPTO_CPS_00.txt

[19] Cryptolib utilise toutes les ressources (NomLAD) déclarées dans le fichier galss.ini dont le nom **commence par CPS**. Si l'on veut utiliser plusieurs lecteurs, chacun doit donc s'appeler CPSxxx. Attention : les noms d'alias ne sont pas pris en compte par Crytolib !

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5.2. AIDES AUX DIAGNOSTICS

En cas de dysfonctionnement, il faut différencier si le problème (ou sa source) vient des bibliothèques CRYPTOLIB-CPS ou des couches en dessous (API-CPS ; GALSS ; lecteur ; carte).

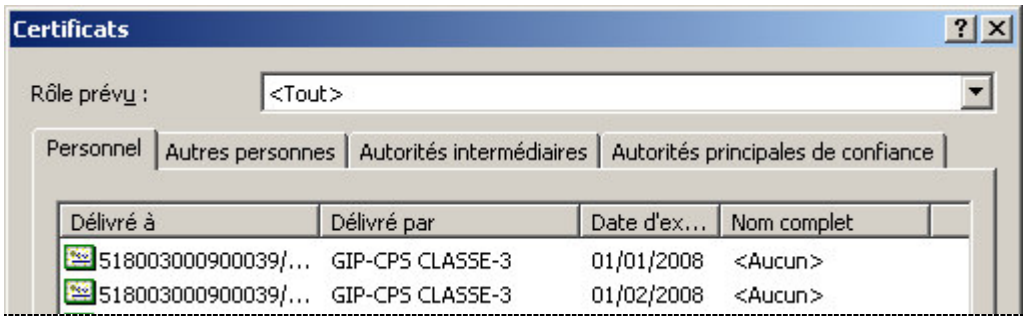
1. Une première approche consiste à lancer le programme de gestion de la CPS :

   Exemple Windows : menu « Démarrer » ; « Programmes » ; « Cryptolib CPS» ; « Gestionnaire de la carte CPS » ou « double-click » sur cpgesw32.exe dans %WINDIR%

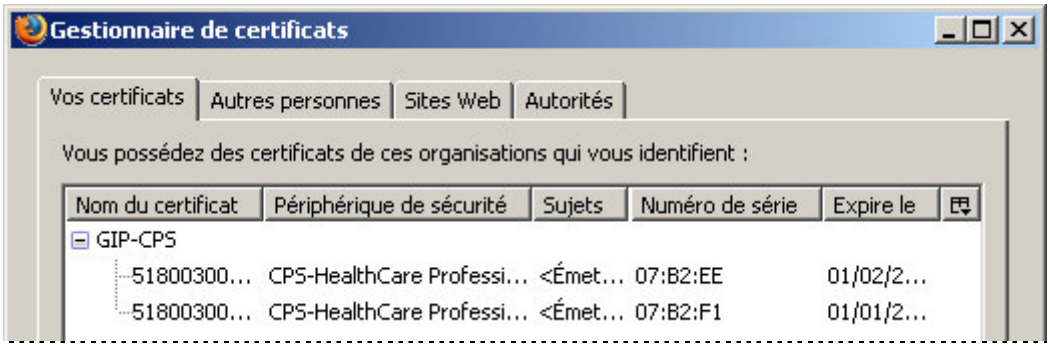
   Si ce programme de gestion de la CPS parvient à afficher les données de votre carte CPS, les couches (API-CPS ; GALSS ; lecteur ; carte) sont en bon état. Sinon, ce programme et son fichier de traces CPS-TRAC.TXT permettront d'affiner le diagnostic (cf. son manuel utilisateur).

2. Si les connexions HTTPS décrites aux chapitres 4.1 et 4.3 ne fonctionnent pas, on peut vérifier si les bibliothèques CRYPTOLIB-CPS détectent bien la carte CPS et lisent bien les certificats X.509. Si ce test est positif, l'anomalie vient plutôt d'un problème entre le serveur auquel vous vous connectez et votre carte CPS.

   Exemples :
   a) Sous Internet Explorer, les menus « Outils » ; « Options Internet… » ; « Contenu » ; « Certificats » doivent visualiser vos deux certificats de votre CPS :



   b) Sous Firefox, les menus « outils » ; « options » ; « Avancé » ; « Certificats » ; « Gérer les certificats » doivent visualiser vos deux certificats de votre CPS :



   En cas d'échec, un diagnostic avancé consistera à vérifier les logiciels installés sur votre poste.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

3. Contrôles des fichiers logiciels installés :

Environnement : Composant et Fichiers	Windows	Linux	MacOSX
GALSS[20] = gestionnaire d'accès aux lecteurs	Dans %WINDIR%	Dans « /usr/local/galss »	Dans « /Library/Frameworks »
GestionClient InformationPoste GALSS ProtocolePCSC ProtocolePSS	galclw32.dll galinw32.dll galssw32.dll pcscw32.dll pssinw32.dll	libgalcllux.so libgalinlux.so libgalsslux.so libpcsclux.so libpssinlux.so	galclosx.framework galinosx.framework galssosx.framework pcscosx.framework pssinosx.framework
			Dans « /Library/Preferences »
Configuration	galss.ini	galss.ini io_comm.ini	galss.ini io_comm.ini
			Dans « /Library/Application Support/Galss »
GestionServeur	galsvw32.exe	galsvlux	galsvosx
API-CPS = Services de la CPS	Dans %WINDIR%	Dans « /usr/local/galss »	Dans « /Library/Frameworks »
GestionCarteCPS GestionDictionnaire OS-Dépendant…	cpsw32.dll cptabw32.dll sscasw32.dll	libcpslux.so libcptablux.so libsscaslux.so	cpsosx.framework cptabosx.framework sscasosx.framework
			Dans « /Library/Preferences »
Dictionnaire	DICO-FR.GIP	DICO-FR.GIP	DICO-FR.GIP
			Dans « /Applications »
Application de Gestion de la CPS	cpgesw32.exe	cpgeslux	cpgesosx iocomcnf

[20] Remarque : sur un poste déjà équipé d'un lecteur et d'une solution de FSE, le setup Cryptolib par défaut ne modifie pas la couche GALSS. Seules les couches API-CPS et Cryptolib sont mises à jour dans ce cas. Pour forcer la mise à jour du composant GALSS, supprimez ou renommez le fichier galss.ini existant avant de lancer l'installation.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Environnement : Composant et Fichiers	Windows	Linux	MacOSX
CRYPTOLIB	Dans %WINDIR%	Dans « /usr/local/galss »	Dans « /usr/lib »
PKCS#11-CPS	cps_pkcs11_w32.dll	libcps_pkcs11_lux.so	libcps_pkcs11_osx.dylib
		Dans « /CryptolibCPS »	Dans «/Library/Preferences»
Configuration	cps_pkcs11_safe.ini	cps_pkcs11_safe.ini	cps_pkcs11_safe.ini
	Dans %WINSYS%		
CSP-CPS	cps_csp_w32.dll cps_csp_w32.sig		
	Dans « C:\Program Files\Cryptolib CPS »		
Extension CSP	CCM.exe		
			Dans « /System/Library /Security/tokend »
Tokend CDSA			GIP-CPS.tokend
			Dans « /usr/libexec /SmartCardServices /driver »
Driver PC/SC sur lecteur PSS			GALSSdriver.bundle
			Dans « /private/etc »
Configuration du driver			reader.conf[21]

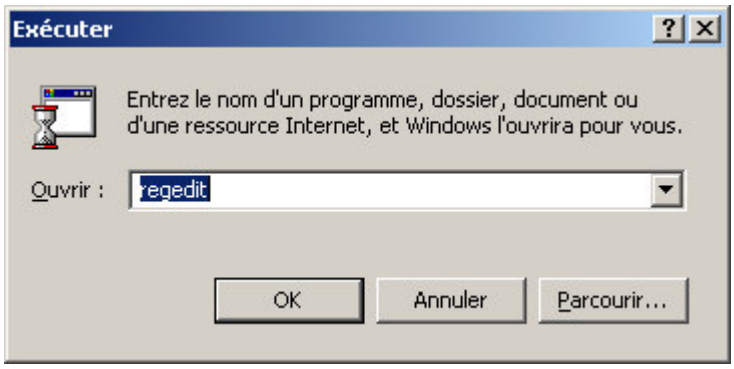
[21] La présence de ce fichier reader.conf dans /private/etc est indispensable pour une utilisation du navigateur Safari avec des lecteurs bi-fentes PSS. Ce fichier doit en revanche être renommé en reader.gip ou supprimé pour une utilisation avec des lecteurs PC/SC. Une utilisation avec une configuration de lecteurs mixte PSS+PC/SC est à proscrire.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

4. Particularités Windows : la « registry » :

cps_csp_w32.dll et sa signature doivent avoir été ajoutées dans la « registry » (base de registres) à l'entrée suivante :

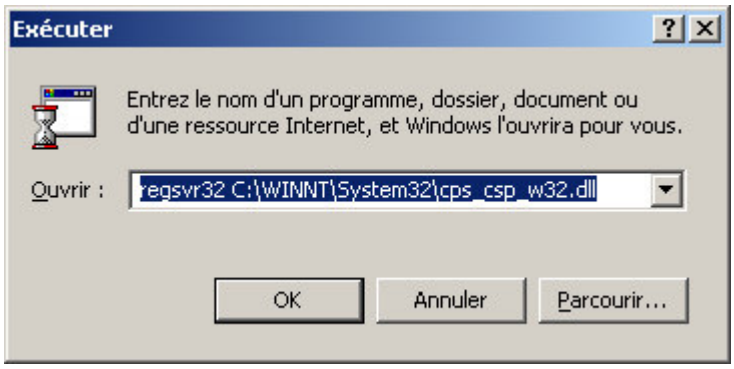
Menu "Démarrer" ; "Exécuter



HKEY_LOCAL_MACHINE\
SOFTWARE\
Microsoft\
Cryptography\
Defaults\
Provider\
cps_csp_w32

Au besoin, les ajouter :

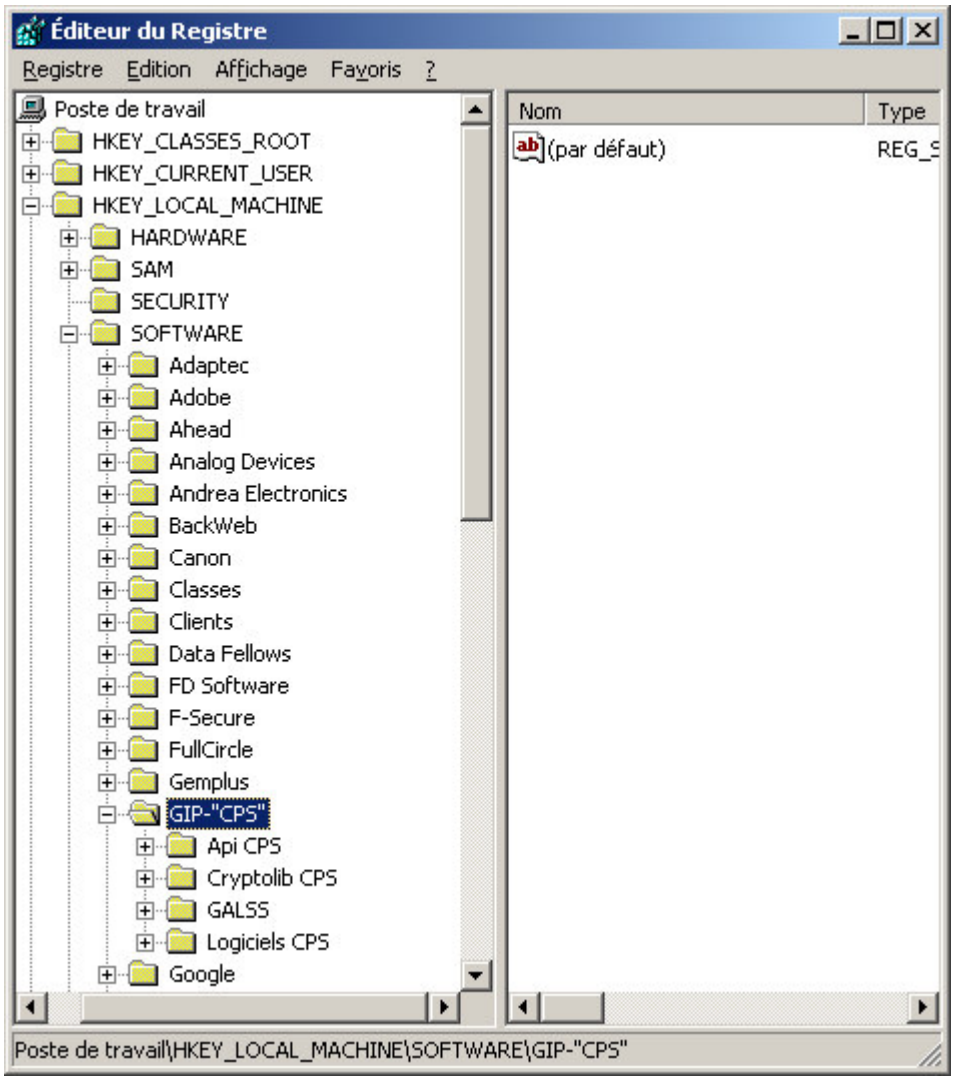
Menu "Démarrer" ; "Exécuter



© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

L'installation a créé les clés suivantes :

HKEY_LOCAL_MACHINE\
SOFTWARE\
GIP-"CPS"\



Enfin, l'installation gère un fichier INSCPSST.INI pour mémoriser ses diverses étapes.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5. Paramétrisation :

Le fichier **cps_pkcs11_safe.ini** permet de configurer Cryptolib.
La section « config » regroupe en particulier les clés permettant de faire des ajustements sur le fonctionnement des différents modules composant Cryptolib.

Ci-dessous la liste des sections et clés permettant de configurer le module Cryptolib :

[Section]	Clé	Défaut	Effet
[config][22]			
	tpc_polling_time	1	Délai en secondes entre 2 tests de présence carte effectif
	cps_open_session_max_try	10	Nombre maximum de tentatives d'ouverture de session CPS
	cps_busy_reader_max_try	10	Nombre maximum de tentatives consécutives d'appel à une fonction CPS qui retourne un CR « lecteur occupé »
	cps_busy_reader_try_sleep	1000	Délai en milliseconde entre deux tentatives consécutives d'appel à une fonction CPS qui retourne un CR « lecteur occupé »
[help]			
	count	0	0 Pas de coffres-forts en mode secours
[safe]			
	directory	…/coffre	Répertoire des coffres-forts
[trace]			
	directory	…/traces	Répertoire des traces
	level	0	0 : Pas de traces 50 : Trace de niveau DEBUG 100 : Traces de niveau MAX

[22] Cette section [config] est facultative et peut être absente du fichier de configuration. Ce sont alors les valeurs par défaut indiquées dans ce tableau qui sont utilisées par le module Cryptolib.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

6. Emplacement des fichiers de trace de la Cryptolib et de CPS-Gestion :

Lorsque l'on quitte CPS-Gestion en sauvegardant certains fichiers journaux (`CPS-JOUR.TXT`, `CPS-INFO.TXT`, `CPS-DIAG.TXT`, `CPS-TRAC.TXT`), ou lorsque les traces de la Cryptolib ont été activées (clé *level* dans la section [trace] du fichier de configuration **cps_pkcs11_safe.ini** décrit ci-dessus), leur emplacement par défaut est le suivant :

Windows :

- Jusqu'au setup Cryptolib v **3.04** inclus :

  `C:\Program files\Cryptolib CPS\traces`

- A partir du setup Cryptolib v **3.06** :

  - sous Windows XP ou 2000[23] :

  `C:\Documents and settings\All Users\Application Data\santesocial\cps\log`

  - sous Windows Vista ou Seven[24] :

  `C:\ProgramData\santesocial\CPS\log`

Mac OS X :

`/Library/Logs/santesocial/CPS`

Linux :

- Fichiers traces de la Cryptolib :

  `/usr/local/cryptolibCPS/traces`

- Fichiers journaux de CPS-Gestion (jusqu'à la v **3.04** incluse) :

  Répertoire d'exécution de CPS-Gestion. Par défaut : `/usr/local/galss`

- Fichiers journaux de CPS-Gestion (v **3.06** et supérieures) :

  `/var/opt/santesocial/CPS/log`

[23] **`Application Data`** est un dossier caché par défaut sous Windows XP et Windows 2000

[24] **`ProgramData`** est un dossier caché par défaut sous Windows Vista et Windows Seven

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5.3. LISTE DES COMPOSANTS INSTALLES

Ce chapitre fournit à titre d'information[25] la liste et les numéros de version de tous les fichiers susceptibles d'être installés ou mis à jour sur le poste, en fonction des différentes versions du programme d'installation (setup) dans les différents environnements.

5.3.1. Environnement Windows

[25] Liste non exhaustive et susceptible d'évolutions.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

- **Liste des composants après installation du setup V 03.04 :**

Composant *emplacement*	Version	Taille du fichier
GALSS V. 3.22 - détail :		
galsvw32.exe *%WINDIR%*	03.21	60 Ko (61 440 o)
galclw32.dll *%WINDIR%*	03.21	64 Ko (65 536 o)
galinw32.dll *%WINDIR%*	03.21	60 Ko (61 440 o)
galssw32.dll *%WINDIR%*	03.22	96 Ko (98 304 o)
pcscw32.dll *%WINDIR%*	03.22	92 Ko (94 208 o)
pssinw32.dll *%WINDIR%*	03.21	112 Ko (114 688 o)
galss.ini *%WINDIR%*	N/A	N/A
APIs V. 5.04 – détail :		
cpsw32.dll *%WINDIR%*	05.04	224 Ko (229 376 o)
cptabw32.dll *%WINDIR%*	05.04	88 Ko (90 112 o)
sscasw32.dll *%WINDIR%*	05.04	80 Ko (81 920 o)
jnicpsw32.dll *%WINDIR%*	05.04	112 Ko (114 688 o)
DICO-FR.GIP *%WINDIR%*	01.20[26]	23,7 Ko (24 350 o)
Applications / Setup – détail :		
cpgesw32.exe (CPS-Gestion) *%WINDIR%*	05.04	412 Ko (421 888 o)
inscpsst.ini *%WINDIR%*	N/A	N/A
Cryptolib – détail :		
cps_pkcs11_w32.dll *%WINDIR%*	01.13	1,19 Mo (1 249 280 o)
cps_pkcs11_safe.ini *%WINDIR%*	N/A	143 o (143 o)
cps_csp_w32.dll *%WINSYS%*	01.22	168 Ko (172 032 o)
cps_csp_w32.sig *%WINSYS%*	N/A	136 o (136 o)
CCM.exe C:\Program Files\Cryptolib CPS	02.03	236 Ko (241 664 o)

[26] Attention : n° de version interne au fichier (fichier texte : pas de version « Windows » sur ce type de fichier).

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

- **Liste des composants après installation du setup V 03.06 :**

Composant *emplacement*	Version	Taille du fichier
GALSS V. 3.26 - détail :		
galsvw32.exe *%WINDIR%*	03.26	68 Ko (69 632 o)
galclw32.dll *%WINDIR%*	03.25	28 Ko (28 672 o)
galinw32.dll *%WINDIR%*	03.21	60 Ko (61 440 o)
galssw32.dll *%WINDIR%*	03.26	96 Ko (98 304 o)
pcscw32.dll *%WINDIR%*	03.22	92 Ko (94 208 o)
pssinw32.dll *%WINDIR%*	03.25	112 Ko (114 688 o)
galss.ini *%WINDIR%*	N/A	N/A
APIs V. 5.05 – détail :		
cpsw32.dll *%WINDIR%*	05.05	224 Ko (229 376 o)
cptabw32.dll *%WINDIR%*	05.04	88 Ko (90 112 o)
sscasw32.dll *%WINDIR%*	05.05	80 Ko (81 920 o)
jnicpsw32.dll *%WINDIR%*	05.04	112 Ko (114 688 o)
DICO-FR.GIP *%WINDIR%*	01.21[27]	24,1 Ko (24 736 o)
Applications / Setup – détail :		
cpgesw32.exe (CPS-Gestion) *%WINDIR%*	05.07	412 Ko (421 888 o)
inscpsst.ini *%WINDIR%*	N/A	N/A
Cryptolib – détail :		
cps_pkcs11_w32.dll *%WINDIR%*	01.17	1,31 Mo (1 380 352 o)
cps_pkcs11_safe.ini *%WINDIR%*	N/A	173 o (173 o)
cps_csp_w32.dll *%WINSYS%*	01.24	300 Ko (307 200 o)
cps_csp_w32.sig *%WINSYS%*	N/A	136 o (136 o)
CCM.exe C:\Program Files\Cryptolib CPS	02.03	236 Ko (241 664 o)

[27] Attention : n° de version interne au fichier (fichier texte : pas de version « Windows » sur ce type de fichier).

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5.3.2. Environnement Macintosh

- **Liste des composants après installation du setup V 03.12 (Universal) :**

Composant */emplacement*	Version OS (info.plist)	Version interne (CPS-Gestion)	Taille et Date de création (E = exécutable au sein du framework)	Type
GALSS V. 3.24 - détail :				
galsvosx */Library/Application Support/Galss*	N/A	3.24	60 Ko (57 696 o) 02/02/09 11:59	Univ.
galclosx.framework */Library/Frameworks*	3.24	3.24	E : 56 Ko (56 692 o) 02/02/09 11:59	Univ.
galinosx.framework */Library/Frameworks*	3.20	3.20	E : 40 Ko (38 660 o) 02/02/09 11:59	Univ.
galssosx.framework */Library/Frameworks*	3.24	3.24	E : 116 Ko (115 308 o) 02/02/09 11:59	Univ.
pcscosx.framework */Library/Frameworks*	3.22	3.22	E : 84 Ko (85 112 o) 02/02/09 11:59	Univ.
pssinosx.framework */Library/Frameworks*	3.22	3.22	E : 120 Ko (122 140 o) 02/02/09 11:59	Univ.
io_comm.ini */Library/Preferences*	N/A	N/A	N/A	N/A
galss.ini */Library/Preferences*	N/A	N/A	N/A	N/A
APIs V. 5.11 – détail :				
cpsosx.framework */Library/Frameworks*	5.11	5.11	E : 432 Ko (439 336 o) 02/02/09 11:59	Univ.
cptabosx.framework */Library/Frameworks*	5.10	N/A	E : 92 Ko (92 536 o) 02/02/09 11:59	Univ.
sscasosx.framework */Library/Frameworks*	5.11	5.11	E : 48 Ko (48 192 o) 02/02/09 11:59	Univ.
libJniCpsosx.jnilib */Library/Java/Extensions*	N/A	N/A	156 Ko (157 188 o) 02/02/09 11:59	Univ.
DICO-FR.GIP */Library/Preferences*	N/A	01.21 du 16/02/09	28 Ko (24 736 o) date install…	N/A
Applications – détail :				
CPS-Gestion */Applications*	05.12 (info.plist)	5.12	E : 224 Ko (228 540 o) 02/02/09 11:59	Univ.
IOCOMCNF */Applications*	5.10 (info.plist)	N/A	E : 56 Ko (57 104 o) 02/02/09 11:59	Univ.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Cryptolib V. 02.02 – détail :				
libcps_pkcs11_osx.dylib */usr/lib*	N/A	N/A	1,8 Mo (1 878 748 o) 02/02/09 11:59	Univ.
cps_pkcs11_safe.ini */Library/Preferences*	N/A	N/A	N/A	N/A
Tokend CDSA – détail :				
GALSSdriver.bundle */usr/libexec/SmartCardServices/drivers*	02.00	N/A	E : 44 Ko (42 672 o) 02/02/09 11:59	Univ.
reader.conf /private/etc	N/A	N/A	N/A	N/A
GIP-CPS.tokend /System/Library/Security/tokend	3.01	N/A	E : 492 Ko (499 820 o) 02/02/09 11:59 E_dbg : 1,4 Mo (1 427 684 o) 02/02/09 11:59	Univ.
Setup – détail :				
inscpsst.ini */Applications*	N/A	N/A	N/A	N/A
ApiCPS.pkg */Library/Receipts*	5.11	N/A	E : 40 Ko (39 482 o) 02/02/09 11:59	N/A
CryptolibCPS.pkg */Library/Receipts*	2.02	N/A	E : 40 Ko (40 036 o) 02/02/09 11:59	N/A
Galss.pkg */Library/Receipts*	3.22	N/A	E : 60 Ko (60 096 o) 02/02/09 11:59	N/A
TokendCPS.pkg */Library/Receipts*	3.01	N/A	E : 36 Ko (36 649 o) 02/02/09 11:59	N/A

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

- **Liste des composants après installation du setup V 03.15 (Universal/64bits) :**

Composant ***/emplacement***	**Version OS (info.plist)**	**Version interne (CPS-Gestion)**	**Taille et Date de création (E = exécutable au sein du framework)**	**Type**
GALSS V. 3.27 - détail :				
galsvosx */Library/Application Support/Galss*	N/A	3.26	90 Ko (86 720 o) 21/02/11 16:51	Univ.
galclosx.framework */Library/Frameworks*	3.27	3.27	E : 94 Ko (90 144 o) 21/02/11 16:51	Univ.
galinosx.framework */Library/Frameworks*	3.26	3.26	E : 61 Ko (59 200 o) 21/02/11 16:51	Univ.
galssosx.framework */Library/Frameworks*	3.27	3.27	E : 180 Ko (177 944 o) 21/02/11 16:51	Univ.
pcscosx.framework */Library/Frameworks*	3.26	3.26	E : 127 Ko (126 520 o) 21/02/11 16:51	Univ.
pssinosx.framework */Library/Frameworks*	3.26	3.26	E : 188 Ko (186 680 o) 21/02/11 16:51	Univ.
io_comm.ini */Library/Preferences*	N/A	N/A	N/A	N/A
galss.ini */Library/Preferences*	N/A	N/A	N/A	N/A
APIs V. 5.14 – détail :				
cpsosx.framework */Library/Frameworks*	5.14	5.14	E : 676 Ko (674 096 o) 24/06/11 09:41	Univ.
cptabosx.framework */Library/Frameworks*	5.11	N/A	E : 131 Ko (129 600 o) 24/06/11 09:41	Univ.
sscasosx.framework */Library/Frameworks*	5.13	5.13	E : 70 Ko (69 144 o) 24/06/11 09:41	Univ.
libJniCpsosx.jnilib */Library/Java/Extensions*	N/A	N/A	238 Ko (234 880 o) 24/06/11 09:42	Univ.
DICO-FR.GIP */Library/Preferences*	N/A	01.21 du 16/02/09	29 Ko (24 736 o) date install…	N/A
Applications – détail :				
CPS-Gestion */Applications*	5.15	5.15	E : 369 Ko (366 624 o) 24/06/11 09:41	Univ.
IOCOMCNF */Applications*	5.10	N/A	E : 49 Ko (47 316 o) 24/06/11 09:41	Univ.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

Cryptolib V. 2.04 – détail :				
libcps_pkcs11_osx.dylib */usr/lib*	N/A	2.04	766 Ko (763 352 o) 10/02/11 15:39	Univ.
cps_pkcs11_safe.ini */Library/Preferences*	N/A	N/A	N/A	N/A
Tokend CDSA – détail :				
GALSSdriver.bundle */usr/libexec/SmartCardServices/drivers*	2.01	N/A	E : 70 Ko (67 832 o) 21/06/11 14:58	Univ.
reader.conf /private/etc	N/A	N/A	N/A	N/A
GIP-CPS.tokend /System/Library/Security/tokend	3.03	N/A	E : 1,3 Mo (1 298 224 o) 21/06/11 14:58	Univ.
Setup – détail :				
inscpsst.ini */Applications*	N/A	N/A	N/A	N/A
ApiCPS.pkg */Library/Receipts*	5.14	N/A	N/A	N/A
CryptolibCPS.pkg */Library/Receipts*	2.04	N/A	N/A	N/A
Galss.pkg */Library/Receipts*	3.27	N/A	N/A	N/A
TokendCPS.pkg */Library/Receipts*	3.03.01	N/A	N/A	N/A

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

5.3.3. Environnement Linux

- **Liste des composants après installation du setup V 03.04 :**

Composant ***/emplacement***	**Version interne (CPS-Gestion)**	**Taille du fichier**
GALSS V. 3.22 - détail :		
galsvlux (exécutable) */usr/local/galss*	3.10	31 Ko (31 523 o)
libgalcllux.so */usr/local/galss*	3.21	24 Ko (24 606 o)
libgalinlux.so */usr/local/galss*	3.07	18 Ko (18 112 o)
libgalsslux.so */usr/local/galss*	3.22	63 Ko (63 555 o)
libpcsclux.so */usr/local/galss*	3.22	38 Ko (38 757 o)
libpssinlux.so */usr/local/galss*	3.22	65 Ko (65 589 o)
io_comm.ini */usr/local/galss*	N/A	N/A
galss.ini */usr/local/galss*	N/A	N/A
APIs V. 5.04 – détail :		
libcpslux.so */usr/local/galss*	5.04	241 Ko (245 866 o)
libcptablux.so */usr/local/galss*	N/A	46 Ko (46 483 o)
libsscaslux.so */usr/local/galss*	5.02	23 Ko (23 464 o)
DICO-FR.GIP */usr/local/galss*	01.20 du 08/04/08	24 Ko (24 350 o)
Applications – détail :		
cpgeslux */usr/local/galss*	5.04	112 Ko (114 681 o)
Cryptolib V. 01.13 – détail :		
libcps_pkcs11_lux.so */usr/local/galss*	N/A	1,1 Mo (1 101 174 o)
cps_pkcs11_safe.ini */usr/local/cryptolibCPS*	N/A	N/A

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

- **Liste des composants après installation du setup V 03.06 :**

Composant ***/emplacement***	**Version interne**	**Taille du fichier**
GALSS V. 3.27 - détail :		
galsvlux (exécutable) */usr/local/galss*	3.26	33,5 Ko (34 337 o)
libgalcllux.so */usr/local/galss*	3.27	25,6 Ko (26 174 o)
libgalinlux.so */usr/local/galss*	3.07	17,7 Ko (18 112 o)
libgalsslux.so */usr/local/galss*	3.27	59,2 Ko (60 607 o)
libpcsclux.so */usr/local/galss*	3.26	37,8 Ko (38 733 o)
libpssinlux.so */usr/local/galss*	3.25	64,2 Ko (65 746 o)
io_comm.ini */usr/local/galss*	N/A	N/A
galss.ini */usr/local/galss*	N/A	N/A
APIs V. 5.06 – détail :		
libcpslux.so */usr/local/galss*	5.06	235,7 Ko (241 395 o)
libcptablux.so */usr/local/galss*	N/A	45,4 Ko (46 483 o)
libsscaslux.so */usr/local/galss*	5.05	23,5 Ko (24 062 o)
DICO-FR.GIP */usr/local/galss*	02.01 du 04/11/10	37,1 Ko (37 985 o)
Applications – détail :		
cpgeslux */usr/local/galss*	5.07	116,2 Ko (118 962 o)
Cryptolib V. 01.16 – détail :		
libcps_pkcs11_lux.so */usr/local/galss*	1.16	1,1 Mo (1 123 317 o)
cps_pkcs11_safe.ini */usr/local/cryptolibCPS*	N/A	N/A

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

6. TERMINOLOGIE

Signification des sigles utilisés dans ce guide :

API	Application Programming Interfaces : bibliothèque de fonctions logicielles.
CAPI	Microsoft Cryptography API (spécifique Microsoft).
CCM	CAPI Certificate Manager : Gestionnaire de certificats CPS.
CDSA	Common Data Security Architecture (spécifique Apple).
CPA / CPE	Carte de Personnel Autorisé / Carte de Personnel d'Etablissement (famille des CPS).
CPS	Carte de Professionnel de Santé.
CryptoLib	Ensemble des composants cryptographiques CPS : librairie PKCS#11, CSP, CCM, TokenD.
CSP	Cryptographic Service Provider (spécifique Microsoft).
HTTPS	Protocole HTTP (Hyper Text Transfert Protocol) Sécurisé.
GALSS	Gestionnaire d'Accès au lecteur Santé Social.
OSM	Outil de messagerie sécurisée.
PC/SC	Personal Computer/Smart Card : standard pour l'intégration des cartes à puce et des lecteurs.
PIN	Personal Identification Number : code de sécurité d'une carte à puce sur 4 chiffres.
PKCS	Public Key Cryptographic Standards: standards de cryptographie à clé publique.
PSS	Protocole Santé Social.
RS232	Port série (ou port COM).
RSA	Algorithme de chiffrement à clef publique et de signature inventé par R.Rivest, A.Shamir et l.Adleman.
TokenD	Module logiciel qui implémente les fonctions CDSA sous environnement Mac.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

7. SUIVI DES MODIFICATIONS DU MANUEL

1. Version 0.1, décembre 2004 : création du manuel d'installation de CRYPTOLIB-CPS.
2. Version 0.2, décembre 2004 :
   - Corrections.
   - Ajout du chapitre 4.1.1 Contrôles sur l'utilitaire CCM.
   - Ajout du chapitre 5 Aides aux diagnostics.
3. Version 0.3, janvier 2005 : Corrections.
4. Version 1.01, février 2005 : Validation.
5. Version 1.02, juin 2005 : Ajout d'appel à regedit & regsvr32 pour enregistrement de la signature du CSP
6. Version 2.00, août 2005 : Prise en compte de la version 2.00 de l'utilitaire d'installation.
7. Version 2.02, septembre 2005 :
   - Prise en compte de la version 2.01 de l'utilitaire d'installation.
   - Remarques du GIE S-V
   - Prise en compte de la version 2.02 de l'utilitaire d'installation
8. Version 2.03, septembre 2006 :
   - Prise en compte du nouveau composant Tokend CDSA dans l'environnement Mac-OSX
   - Ajout du chapitre 5.3 Liste des composants installés
9. Version 2.04, septembre 2006 :
   - Ajout de la liste des composants installés pour l'environnement Macintosh
   - Corrections suite aux remarques de la CNAMTS/WebMédecin
10. Version 2.05, novembre 2006 :
    - Ajout de la liste des composants installés pour l'environnement Linux.
11. Version 2.06, juillet 2007 :
    - Quelques corrections et évolutions, dont l'ajout de la bibliothèque JNI dans les listes de composants installés (Mac et Windows).
12. Version 2.07, octobre 2007 :
    - Chapitre 3 GUIDE D'INSTALLATION de CRYPTOLIB : ajout des remarques sur les droits d'Administrateur et sur les droits d'accès aux répertoires Coffre et Traces.
13. Version 2.08, juin 2008 :
    - Chapitre 5.3 Liste des composants installés : ajout des nouvelles listes des composants installés par les setups V 03.04 (Windows, Linux) et V 03.11 (Mac)
14. Version 2.09, mars 2009 :
    - Chapitre 5.3 Liste des composants installés : ajout de la nouvelle liste des composants installés par le setup V 03.12 pour Macintosh (rem : taille et date des frameworks supprimés car non significatifs + déplacement des lignes galss.ini dans la partie GALSS pour tous les tableaux).
15. Version 2.10, janvier 2010 :
    - Ajouts : version minimale du GALSS sous TSE/Citrix, compatibilité avec MacOS 10.5.x, version Windows Seven et précision UAC, précision configuration Firefox.
16. Version 2.11, mai 2010 :
    - Ajouts : logo et références ASIP, version minimale du setup Cryptolib pour Vista/Seven, liste des composants installés par le setup V 03.06 Windows.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.

17. Version 2.12, novembre 2011 :
    - Chapitre 3.1 : ajout du pré-requis sur l'adresse physique des lecteurs PSS.
    - Chapitre 5.3 : ajout de nouvelles listes des composants installés, et suppression de celles devenues obsolètes.
    - Tous chapitres : ajout d'informations concernant les OS Mac et Linux, et prise en compte des remarques du GIE Sesam-Vitale.
    - Nouveau Chapitre 3.3 : Désinstallation.
    - Nouveau Chapitre 6 : Terminologie.
18. Version 2.13, février 2012 :
    - Chapitre 5.2 Aides aux diagnostics : ajout des emplacements par défaut des fichiers de trace.
    - Chapitre 5.3 Liste des composants installés : ajout de la nouvelle liste des composants installés par le setup V 03.06 pour Linux, et suppression de celle devenue obsolète.

© ASIP Santé : Ce document est la propriété de l'ASIP Santé.
Il ne peut être reproduit sans autorisation écrite.